Windows server i domenski sustav

Lončarić, Viktor

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Stručni studij

WINDOWS SERVER I DOMENSKI SUSTAV

Završni rad

Viktor Lončarić

Osijek, 2019.

SADRŽAJ

1.	Uvod	1
2.	Osnove Windows servera i domenskog sustava	2
3.	Instalacija operacijskog sustava Windows Server 2016 i osnovne postavke	4
4.	Konfiguracija Windows domene	12
5.	Domenski računi	21
6.	Konfiguracija DHCP servera	26
7.	Dodavanje klijentskog računala u domenski sustav	32
8.	Group policy	35
9.	Zaključak	43
10.	Literatura	45
11.	Sažetak	47

1. UVOD

U današnje vrijeme mnoge tvrtke se za svoje poslovanje oslanjanju na upotrebu velikog broja računala. Kako to inače biva, kod velikog broja korisnika i računala je potrebno cijeli taj sustav administrirati. Taj zadatak se uvelike može olakšati spajanjem takvog sustava u lokalnu (LAN) mrežu i dodavanjem servera te instalacijom Windows server operacijskog sustava na isti i podešavanjem domene. U takvom sustavu će klijenti vršiti autentifikaciju na serveru i neće postojati klasični Windows lokalni računi.

Glavna uloga servera je da se ponaša kao *Domain Controller* (DC), što znači da su na serveru pohranjeni svi podaci o korisnicima, njihovim računima i organizacijskoj strukturi potrebni za rad. To za administratora znači da sada ima mogućnost administranja svih domenskih računa s jedne centralne lokacije te da se pomoću ovakvog sustava vrlo jednostavno mogu napraviti promjene koje će se primjeniti na cijeli sustav. Osim uloge AD, server će imati i uloge u mrežnoj infrastrukturi mreže.

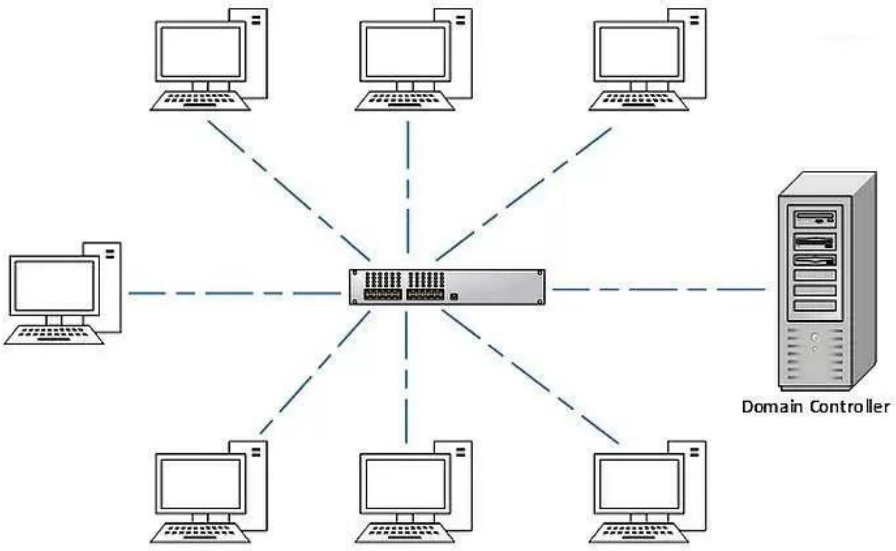
Uzmimo na razmatranje ulogu DNS (*Domain Name System*) servera. DNS uloga služi da bi DNS server mogao „prevesti“ numeričke IP adrese u domenska imena računala, i bez takve uloge u domenskom sustavu komunikacija između klijenta i servera nebi bila moguća. Osim navedenih uloga, server će imati i ulogu DHCP (*Dynamic Host Configuration Protocol*) servera. Takva uloga u sustavu omogućuje automatsko dodjeljivanje dinamičkih IP adresa, te bi u suprotnom svakom računalu u sustavu morali ručno dodjeljivati statičku IP adresu. DHCP server je najlakše shvatiti kao nekakvu „tablicu“ IP adresa, gdje se svakom novom računalu u mreži automatski dodjeljuje prva slobodna dinamička IP adresa iz zadanog opsega.

Problem promjena postavki na velikom broju računala možemo rješiti pomoću *Group Policy*-a (GP). Pomoću ove mogućnosti možemo promjeniti postavke na svim računalima u domeni. Osim promjeni postavki sustava možemo instalirati program na sva računala odjednom s centralne lokacije, možemo korisnicima automatski dodati dijeljeni direktorij, dodati novi pisač, itd. Naravno, navedene su samo neke najčešće primjene GP-a, a mogućnosti su stvarno raznolike. Kao što možemo vidjeti mogućnosti Windows servera i domenskog sustava su stvarno brojne, a ovom radu biti će obrađene mogućnosti i načini postavljanja Windows domenskog sustava, administriranje računa, uspostavljanje hijerarhije u takvom sustavu te već opisane mrežne uloge servera i mogućnosti *Group policy* objekata.

2. OSNOVE WINDOWS SERVERA I DOMENSKOG SUSTAVA

U ovom radu koristit će se Windows server 2016, koji je razvijan usporedno s Windows 10, koji možemo nazvati operacijskim sustavom za općenitu upotrebu. Činjenica da je Windows server 2016 razvijan usporedno s Windows 10 znači da dijele mnoge značajke, kao npr. isto grafičko sučelje (postoji i *command line* verzija Windows servera 2016, odnosno verzija kojoj se upravlja tekstualnim naredbama, ali se nećemo baviti tom verzijom u ovom radu).[1] Još jedna važna sličnost je da Windows server 2016 i Windows 10 imaju istu jezgru, odnosno *kernel*, što omogućuje pokretanje 64-bitne aplikacije prvotno pisane za Windows 10 (ili neke starije verzije Windowsa) na Windows server 2016. U većini slučajeva te se aplikacije ponašaju isto kao i na verzijama Windows operacijskog sustava za koje su namijenjene. Iako dijele mnoge sličnosti, Windows server i Windows 10 imaju i mnoge razlike. Očita je razlika u namjeni, Windows 10 je operacijski sustav namijenjen svakodnevnom korištenju na osobnim računalima dok je Windows server najmanjem korištenju na serveru (kako mu i samo ime govori).[3] Ta razlika se najbolje vidi kada se korisnik s administratorskim pravima prijavi na server, gdje se odmah s prijavom pokreće prozor *Server Manager*-a, koji nije ništa drugo nego program koji služi za upravljanje serverom. Neke od glavnih namjena Windows servera su upravljanje drugim računalima, datotekama, servisima kao i pokretanje servisa kojima korisnici mogu pristupati preko mreže. Da bi konfigurirali i koristili te mogućnosti Windows server sustava koristimo takozvane server *role* (ili uloge). Najvažnija uloga za ovaj rad je *Active Directory Domain Services*, koja omogućuje upravljanje korisnicima i računalima. Ta uloga efektivno pretvara Windows server u *Domain Controller* te nam omogućuje postavljanje i konfiguriranje domene.[2]

Domena je vrsta mreže u kojoj su sva računala (i pripadajući korisnički računi) i eventualna ostala oprema (npr. printeri) registrirani u središnjoj bazi podataka na *Domain Controlleru*. Za upravljanje tom bazom podataka koristimo komponentu Windows servera koja se zove *Active Directory*. *Active Directory* nam omogućuje da računala i korisničke račune koji su članovi domene smjestimo u organizacijske jedinice ovisno o lokaciji, organizacijskoj strukturi određene tvrtke ili o nekim drugim faktorima. Pomoću organizacijske jedinice je moguće organizirati hijerarhiju u bazi podataka.[4]



Slika 2.1. – prikaz jednostavnog domenskog sustava [14]

Na slici 1.1. vidimo grafički prikaz jednostavnog domenskog sustava. Možemo primjetiti kako su klijentska računala povezana s serverom (*Domain Controllerom*) putem *network switcha* odnosno preklopnika. Kada je računalo povezano s serverom možemo ga „dodati" u domenu. Dodavanjem u domenu ostvaruje se mogućnost da se korisnik na računalo prijavi sa svojim domenskim računom, koji je poseban korisnički račun koji se kreira u *Active Directory* sustavu. Važno je napomenuti kako domenski račun nije lokalni račun, te se korisnik s svojim domenskim računom može prijaviti na svako računalo koje je član domene. Autentifikacija se vrši na *Domain Controlleru*, te računalo pri prvoj prijavi „povuče" postavke za određeni korisnički račun i stvori lokalnu verziju računa s prije podešenim postavkama.[6]

Suprotnost domeni je *Windows Workgroup*. *Workgroup* je model grupiranja računala u okruženju gdje ne postoji domena, gdje se smatra da su računala „samostalna", odnosno rade neovisno o drugom hardwareu ili softwareu. Autentifikacija se odvija lokalno, a računi su također spremljeni lokalno, što znači da se nije moguće prijaviti s istim računom na drugo računalo. U *Workgroupi* nema server-klijent komunikacije, nego se odvija *peer-to-peer* komunikacija, gdje svako računalo komunicira s drugim računalom izravno, bez autentifikacije na nekom serveru. Taj model je zadani model kada instaliramo Windows operacijski sustav na računalo, te je pogodan za kućnu upotrebu ili manje mreže (preporuka do desetak klijenata). [6]

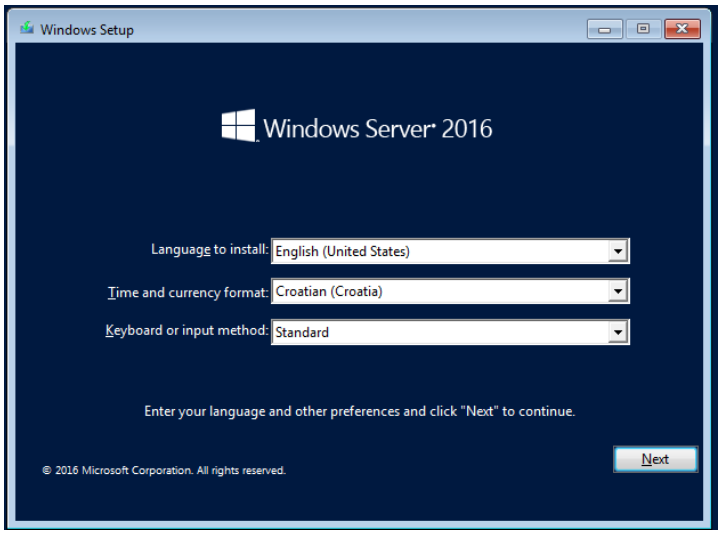
3. INSTALACIJA OPERACIJSKOG SUSTAVA WINDOWS SERVER 2016 I OSNOVNE POSTAVKE

Prije nego što možemo uopće početi s radom na serveru i podešavanjem istog, potrebno je instalirati odgovarajući operacijski sustav (u daljnjem tekstu OS) i podesiti neke osnovne postavke. Za svrhu ovog rada koristit će se evaluacijsko izdanje Windows Server 2016 ver. 1607 OS-a. Slijedi kratko objašnjenje instalacije i podešavanje nekih osnovnih postavki za normalan rad sustava.

U nekakvom idealnom scenariju instalirali bi Windows Server na virtualnu mašinu koja je pokrenuta na nekom fizičkom serveru. Zbog nemogućnosti korištenja pravog, fizičkog servera instalirat ćemo Windows Server 2016 na standardno PC računalo koje zadovoljava sistemske zahtjeve. To računalo će „glumiti" fizički server.

Prije same instalacije potrebno je preuzeti instalacijsku *.iso datoteku koja je dostupna za preuzimanje na služenoj Microsoftovoj stranici. Nakon preuzimanja instalacijske datoteke (u našem slučaju radi se o evaluacijskoj verziji sustava), potrebno je kreirati instalacijski medij. Za potrebe ovog rada poslužit ćemo se USB memorijom. Koristit ćemo *Microsoft Windows USB download tool* kako bi od USB memorije i instalacijske *.iso datoteke napravili bootabilan instalacijski medij.

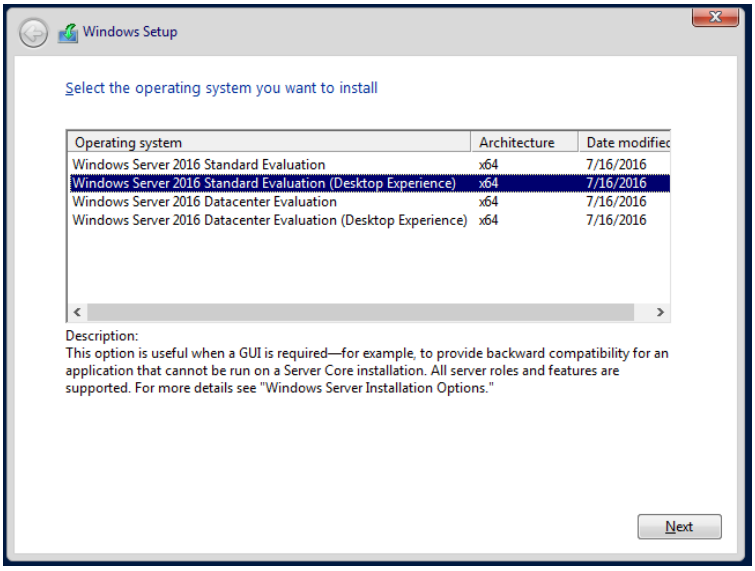
Kada smo napravili instalacijski medij, možemo ga uključiti u USB port u „server" (preporuka je izbjegavati *front panel* i *USB hubove*, te bi USB memoriju bilo idealno uključiti direktno u matičnu ploču s stražnje strane računala). Sada možemo upaliti server. Prije svega je vrlo važno ući u BIOS (ili UEFI) te podesiti *boot* redoslijed tako da USB memorija bude na prvom mjestu. Nakon toga možemo ponovno pokrenuti računalo. Ukoliko je sve pravilno podešeno, na serveru bi se trebao pokrenuti Windows *setup* koji izgleda ovako (Slika 3.1.):



Slika 3.1. – Windows setup

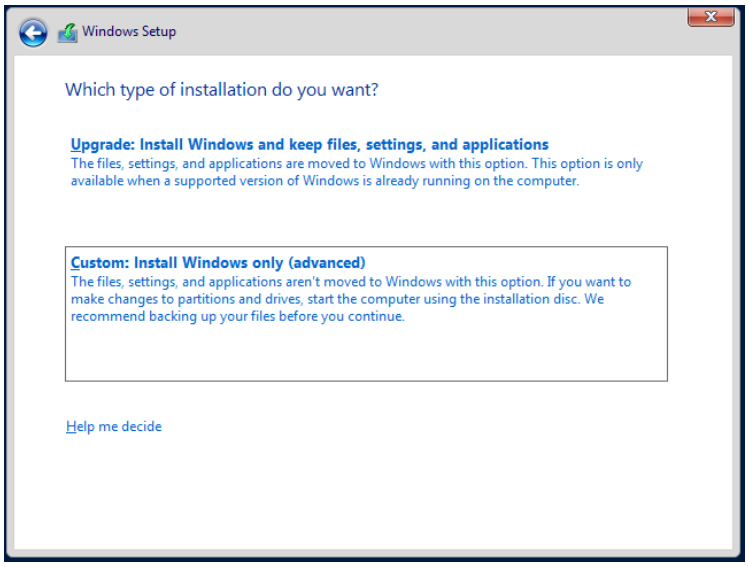
Ukoliko prije imamo bilo kakvog iskustva s instalacijom Windows OS-a, instalacija Windows Servera 2016 će biti vrlo jednostavna. Za razliku od nekih starijih verzija sustava Windows OS-a, tu imamo grafičko sučelje kojim upravljamo mišem. Sam proces instalacije, kao i grafičko sučelje su skoro identični procesu instalacije Windowsa 10, te se povlači pretpostavka da ako korisnik zna instalirati Windows 10 OS, trebao bi moći instalirati i Windows Server 2016 bez poteškoća.

Da bi instalacija započela potrebno je odabrati jezik sustava kojeg želimo instalirati, odrediti regionalne postavke te raspored tipkovnice. U našem slučaju instalirat ćemo Windows Server 2016 na engleskom jeziku s hrvatskim regionalnim postavkama i standardnim rasporedom tipkovnice. Klikom na tipku next otvara se prozor s tipkom *Install now*. Kada kliknemo na *Install now* instalacija započinje, te se od korisnika traži da odabere vrstu OS-a koju želi instalirati (Slika 3.2.):



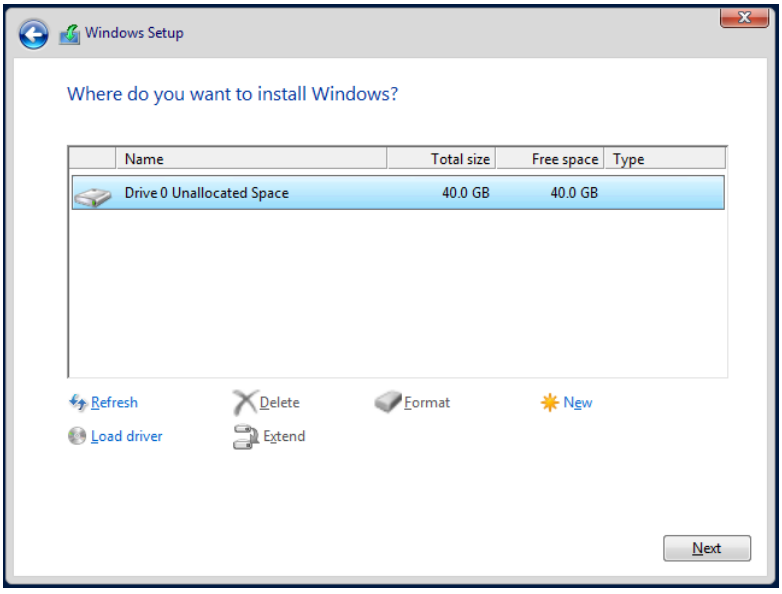
Slika 3.2. – Vrste OS-a

Standardna verzija sustava biti će sasvim dovoljna za potrebe ovog rada, a odabiremo *Desktop Experience* ediciju kako bi imali dostupno grafičko sučelje s kojim je ipak lakše raditi u odnosu na tekstne komande. Pritiskom na tipku *Next* prelazimo na prozor s licencom, koju moramo prihvatiti kako bi mogli nastaviti dalje. Kada smo prihvatili licencu dolazimo do prozora na kojem trebamo izabrati želimo li nadograditi postojeću verziju Windows Server sustava ili želimo svježu, čistu instalaciju (Slika 3.3.):



Slika 3.3. – izbor načina instalacije

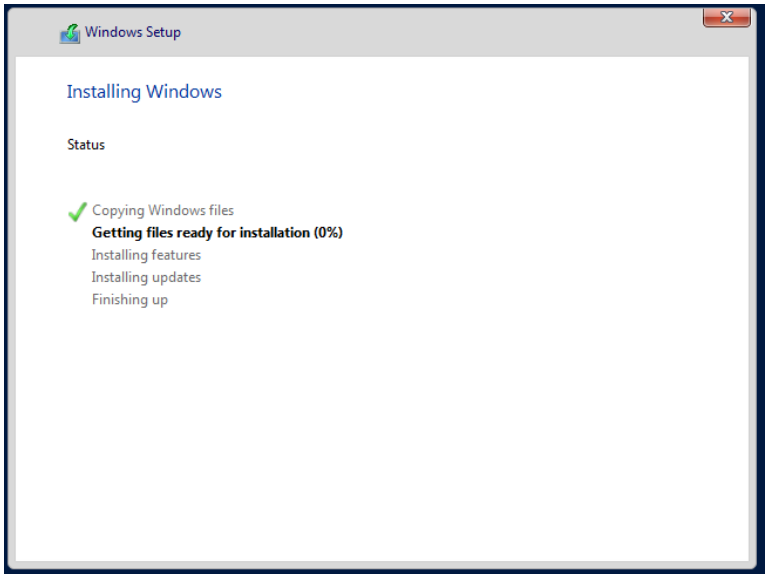
S obzirom kako na serveru trenutno ne postoji niti jedna druga verzija Windows OS-a odabiremo drugu opciju, odnosno svježu instalaciju. Nakon toga je potrebno odabrati na koji disk (ili particiju) želimo instalirati OS, odnosno želimo li kreirati kakve dodatne particije (Slika 3.4.):



Slika 3.4. – odabir mjesta instalacije

Iz slike 2.4 možemo zaključiti kako je disk na serveru potpuno prazan. U ovom slučaju dovoljno je samo označiti *Drive 0* i kliknuti *Next*, a *Windows Setup* automatski kreira jednu sistemsku particiju na disku (koja kasnije nije dostupna korisniku) i jednu lokalnu particiju na koju je instaliran sam OS. Ova particija po zadanim postavkama dobiva slovo C kao oznaku.

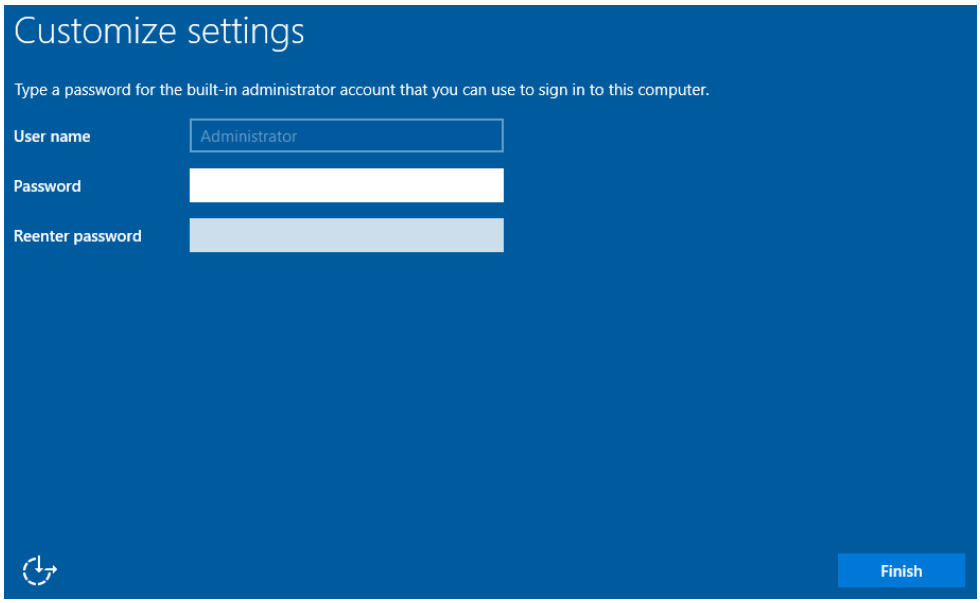
Klikom na *Next* zapravo je završen prvi dio instalacije i pokreće se automatizirani proces kopiranja datoteka na disk, raspakiravanje istih i priprema za instalaciju, instaliranje osnovnih značajki sustava i mogućih ažuriranje te završetak instalacije (koji je velikim dijelom samo brisanje raspakiranih datoteka) (Slika 3.5.):



Slika 3.5. – prozor automatiziranog procesa instalacije

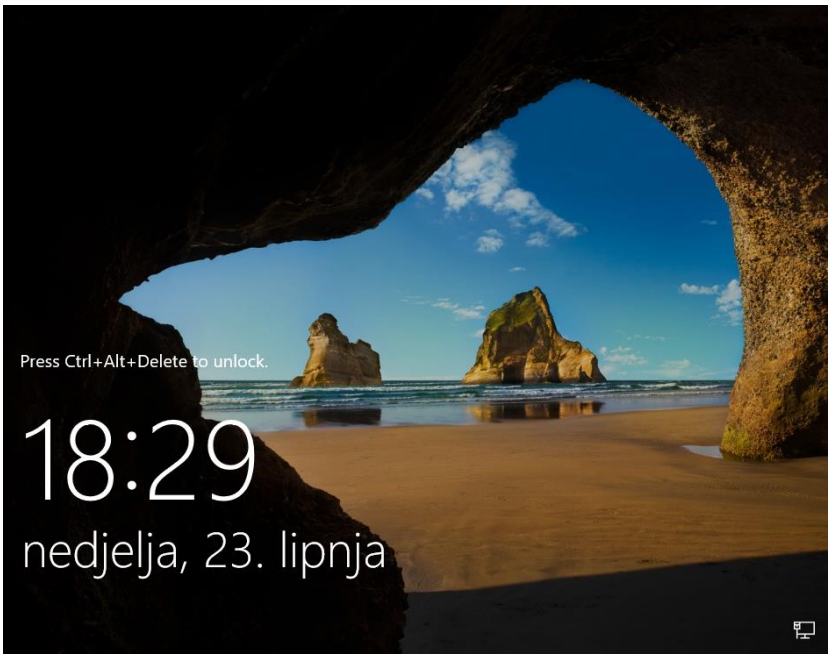
Nakon završetka automatiziranog procesa, računalo se automatski ponovno pokreće.

Nakon što se računalo ponovno pokrenulo, potrebno je podesiti osnovne postavke da bi sustav mogao pravilno i sigurno funkcionirati. Prije svega sustav od korisnika traži da podesi lokalni Administrator račun, odnosno da ga zaštiti lozinkom (Slika 3.6.). Za razliku od Windows 10 OS-a Administrator račun u Windows Server 2016 mora biti zaštićen dovoljno kompleksnom lozinkom (minimalno 8 znakova, veliko slovo i broj).



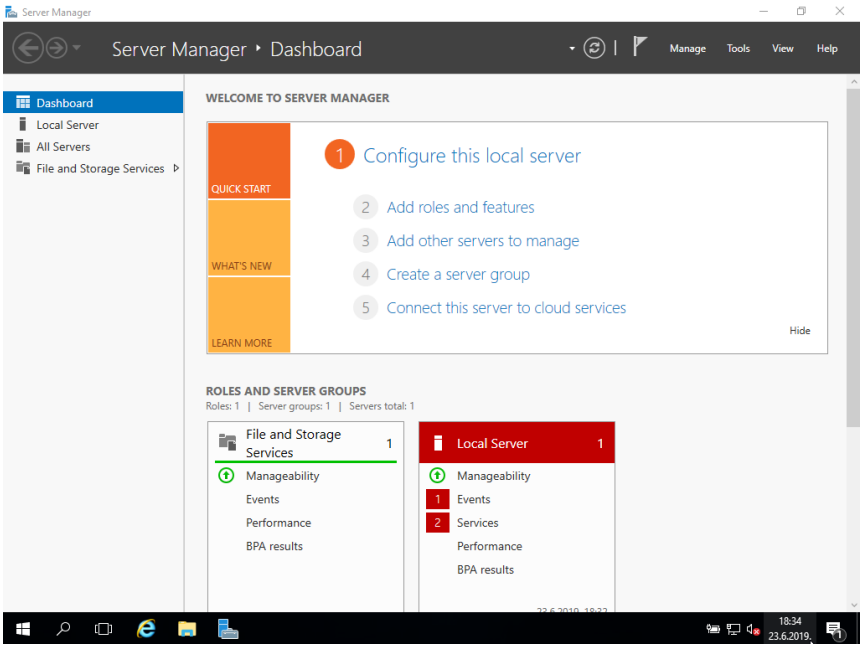
Slika 3.6. – Podešavanje lozinke Administrator računa

Nakon podešavanja Administrator računa instalacija je završila te je na našem serveru uspješno instaliran Windows Server 2016 OS. Ukoliko je sve pravilno instalirano na ekranu trebamo vidjeti „*Windows start screen*“ (Slika 3.7.):



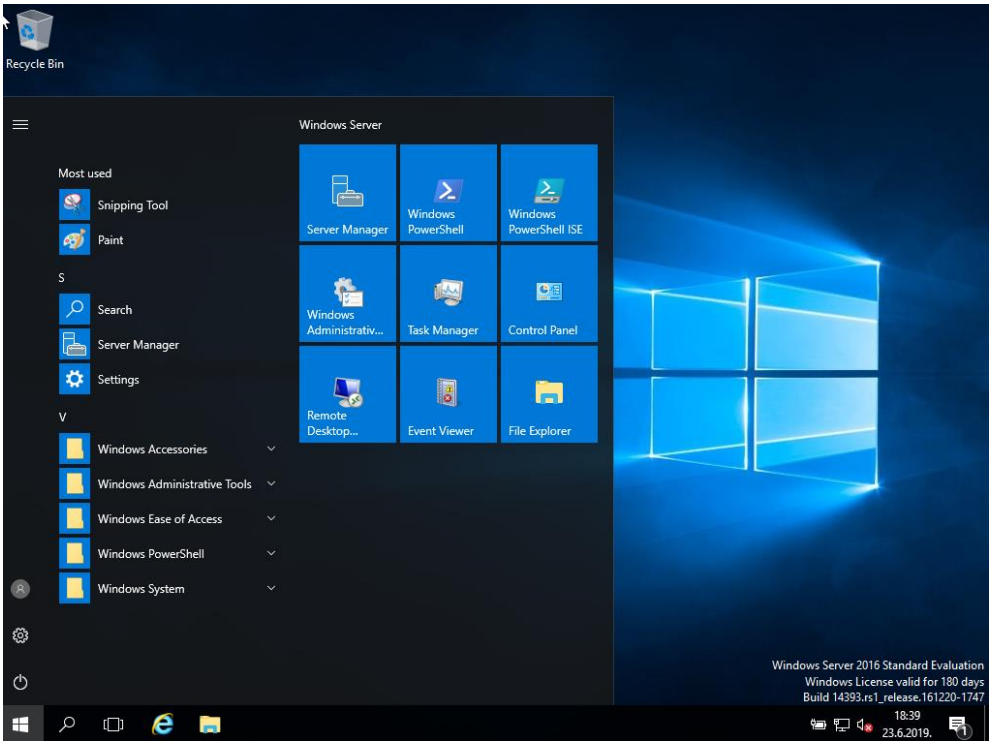
Slika 3.7. – Windows start screen

Pritiskom na kombinaciju tipki *Ctrl+Alt+Delete* računalo je „otključano“, odnosno možemo se prijaviti Administrator računom s lozinkom koju smo postavili u prethodnom koraku. Prijavom na Administrator račun otvara nam se *Server manager* (Slika 3.8.):



Slika 3.8. – Izgled zaslona nakon prve prijave

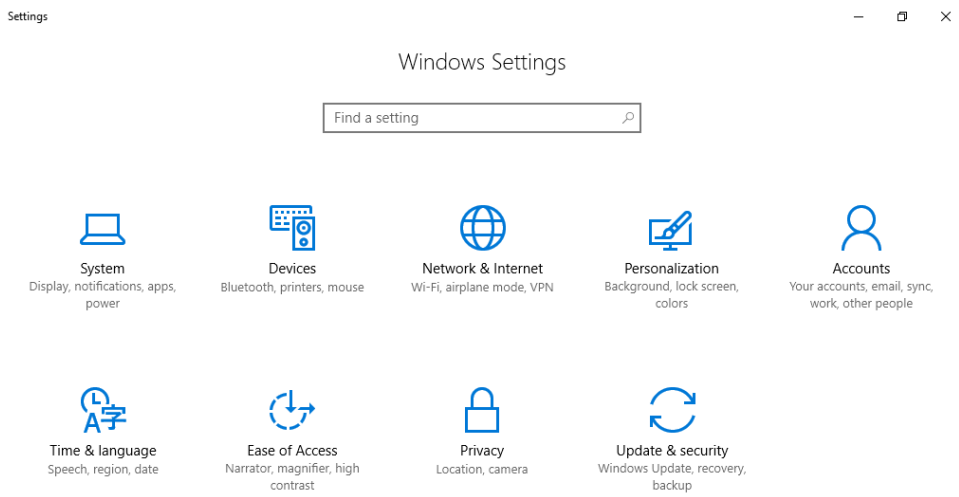
Zasada se još nećemo baviti *Server managerom*, nego ćemo krenuti u osnovno podešavanje samog sustava. Ali prije svega promotrimo grafičko sučelje i izgled radne površine (Slika 3.9.):



Slika 3.9. – Grafičko sučelje Windows Server 2016 OS-a

Možemo primijetiti kako je grafičko sučelje gotovo identično onome na koje smo navikli kod Windowsa 10. Isto tako valja zapaziti kako Windows Server 2016 dolazi s puno manje predinstaliranih aplikacija u usporedbi s Windows 10, što je vidljivo i u izborniku Start.

Krenimo s postavljanjem nekih osnovnih postavki koje su bitne za normalno korištenje samog OS-a. Klikom na ikonu zupčanika u izborniku Start otvara se prozor *Windows Settings* u kojem su sadržane većina postavki (Slika 3.10.):

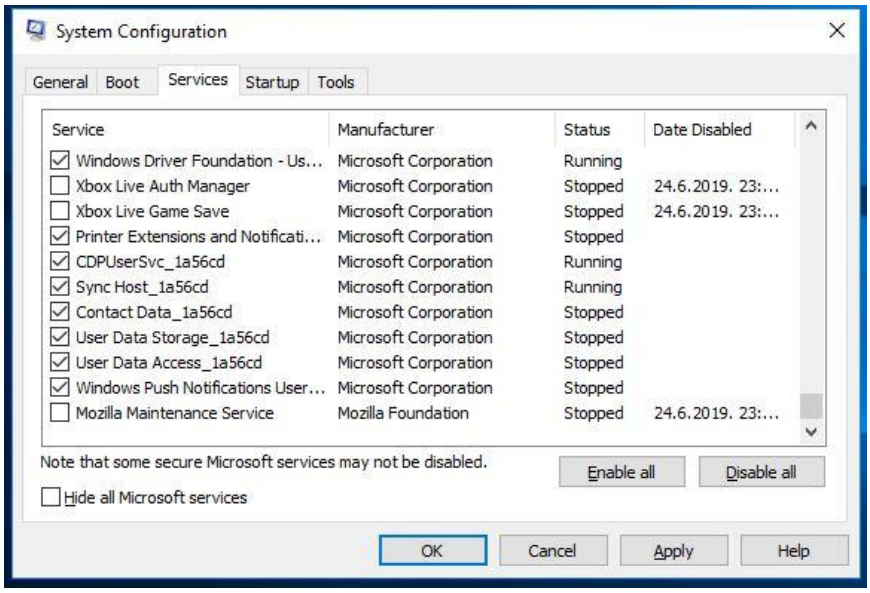


Slika 3.10. – prozor Windows Settings

Postavke možemo naći ručno ulazeći u svaku kategoriju te tako možemo postaviti odgovarajuće vrijednosti, ili možemo upisivati engleski naziv postavki u tražilicu iznad kategorija, koja je vidljiva na slici. Postoji i alternativni način traženja postavki, upisivanjem engleskog naziva u tražilicu start menija, ali ćemo u ovom slučaju koristiti *Windows Settings*.

Osnovne postavke su standardne kao kod instalacije svakog Windows OS-a, ali je zbog posebne namjene servera vrlo važno pravilno postaviti regionalne postavke i postavke vremena i vremenske zone kako bi kasnije izbjegli moguće probleme s kompatibilnosti ili probleme s *Windows Update* servisom. Sam način kako to napraviti je prilično jednostavan te je uvelike olakšan upotrebom *Windows Settings* sučelja. Također treba provjeriti postavke tipkovnice i obratiti pažnju je li raspored tipkovnice pravilno podešen kako bi se izbjegli mogući problemi zbog pogrešnog slova kasnije.

Poželjno je i onemogućiti servise koji nemaju veze s funkcijom servera (u ovom slučaju *Xbox* servisi, telefon, fax i slično). To možemo napraviti u *msconfig* prozoru. Do njega je najlakše doći tako da u pretragu u start meniju jednostavno upišemo *msconfig*, odaberemo *services tab*, kroz njega prođemo ručno i onemogućimo sve nepotrebne servise. (Slika 3.11.)



Slika 3.11. – Services tab

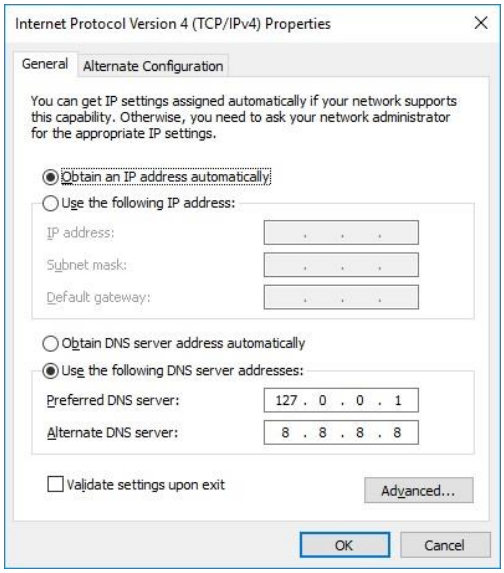
Prije nego što završimo s nekim osnovnim postavkama preporuča se pokrenuti *Windows Update* kako bi provjerili postoji li moguće ažuriranje sustava, te ako postoji preuzeli i instalirali isto.

4. KONFIGURACIJA WINDOWS DOMENE

Nakon instalacije Windows server OS-a na računalo, ovaj „server“ još uvijek nije pravi server zato što nema nikakvu ulogu. Vrijeme je da se serveru dodjeli ulogu *Active Directory Domain Services* te da server postane *Domain Controller* (u daljnjem tekstu DC).

Potrebno je naglasiti da kada postavimo *Active Directory* (u daljnjem tekstu AD) da će server imati i ulogu DNS (*Domain Name System*) servera, bez kojeg funkcioniranje domene nije moguće. DNS je ključan dio domene (i interneta općenito), a njegova uloga je da „prevodi“ numeričke IP adrese u domenske nazive, koje je puno lakše zapamtiti i s kojima je ljudima prirodnije raditi. Uzmimo za primjer adresu 23.32.220.96, koju DNS „prevodi“ kao www.microsoft.com, što je oblik koji je puno lakše zapamtiti. Isto tako DNS je ključan za identifikaciju uređaja i servisa u mreži te ga koriste skoro svi mrežni protokoli. [8]

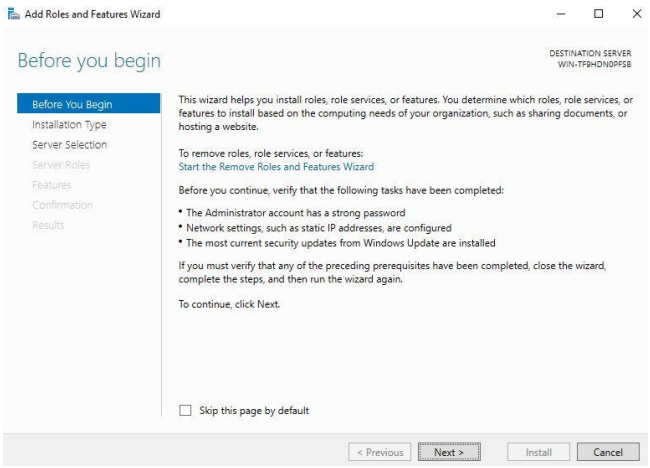
Nakon opisa neke općenite uloge DNS-a jasno je da je njegov zadatak u domeni identifikacija računala i ostalih uređaja koji su u istoj mreži kao i DC. Prije dodjeljivanja uloge AD DC-a, potrebno je postaviti statičku adresu DNS servera. Pošto će DC server ujedno biti i DNS server, adresu DNS-a u postavkama postavljamo na 127.0.0.1, odnosno *localhost* (Slika 4.1.):



Slika 4.1. – DNS postavke servera

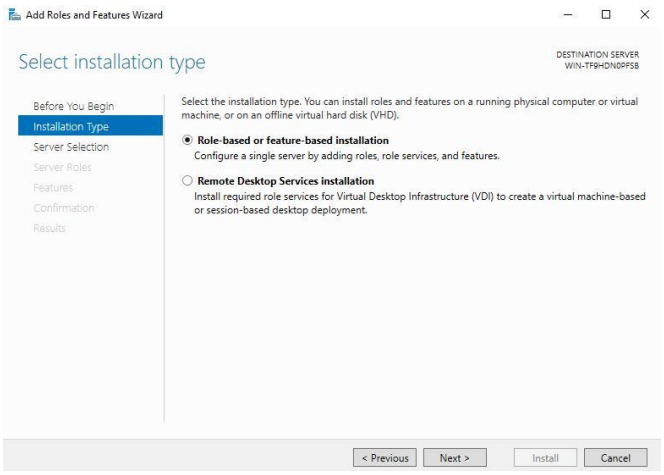
Nakon podešavanja DNS postavke na serveru otvaramo *Server manager*, te kliknemo na *Add roles and features,* te nam se otvara „čarobnjak“ koji nas vodi kroz proces dodjeljivanja nove uloge serveru. U prvom prozoru (Slika 4.2.) su prikazana opća objašnjenja i upozorenja što je potrebno

podesiti prije dodavanja uloga. Pošto smo sve potrebno podesili prije pokretanja čarobnjaka, kliknemo *Next*.



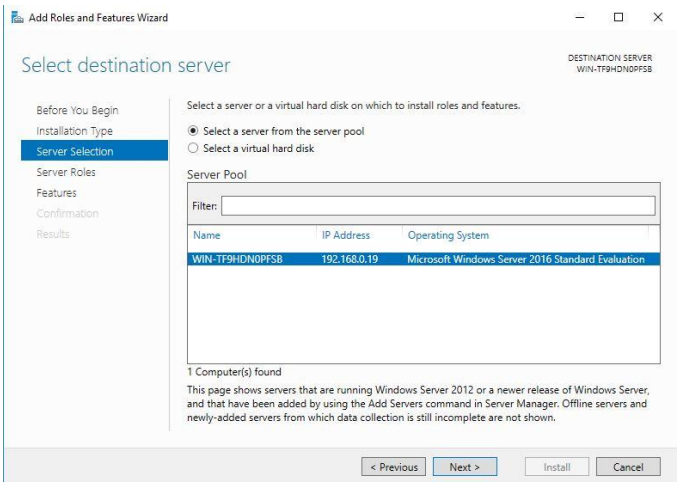
Slika 4.2.. – početni prozor čarobnjaka

Dolazimo do prozora gdje trebamo odabrati tip instalacije (Slika 4.3.). Pošto je ovo jedini lokalni server u mreži ostajemo pri *Role-based or feature-based installation* opciji, te klikamo na *Next*.



Slika 4.3.. – odabir tipa instalacije

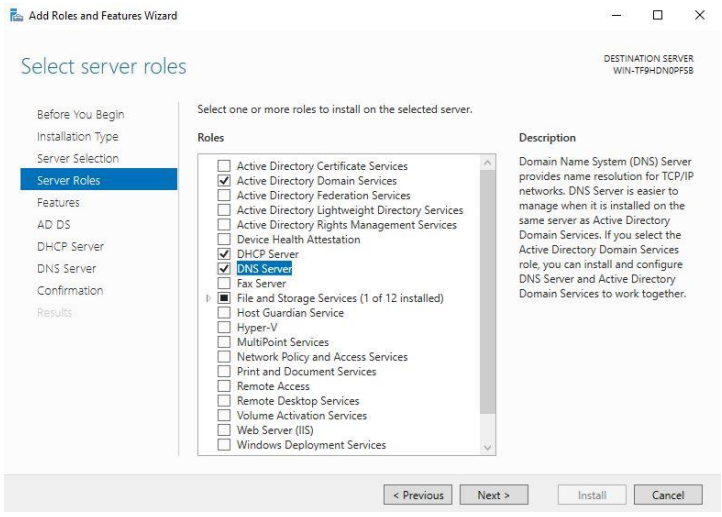
Sada treba odabrati server. Ponovno ostajemo pri zadanoj vrijednosti (Slika 4.4.) zato što je ovo jedini server u mreži.



Slika 4.4. – odabir servera

Dolazimo do najbitnijeg djela ovog procesa, izbora uloga servera. U ovom slučaju odabiremo *Active Directory Domain Services*, *DHCP Server* i *DNS Server* (Slika 4.5.).

Server koji će biti domain controller mora imati i ulogu DNS servera. Uloga DNS servera je ključna da bi uređaji u mreži mogli međusobno komunicirati i da bi mogli pronaći DC.[8] Također, serveru smo dodijelili ulogu DHCP servera zato da izbjegnemo potrebu za ručnim postavljanjem statičkih IP adresa u mreži, a DHCP (*Dynamic Host Configuration Protocol*) protokol nam omogućuje da server s DHCP ulogom automatski dodjeljuje slobodne dinamičke IP adrese u mreži.[9] Ali prije svega serveru dodjeljujemo najvažniju ulogu - *Active Directory Domain Services,* koja nam omogućuje da server postane *Domain Controller*. Možemo primijetiti kako je zadana uloga servera *File and Storage Services*, koja nam omogućuje dijeljenje datoteka koje su spremljene na serveru. To može biti vrlo korisna stavka te će ostati uključena.

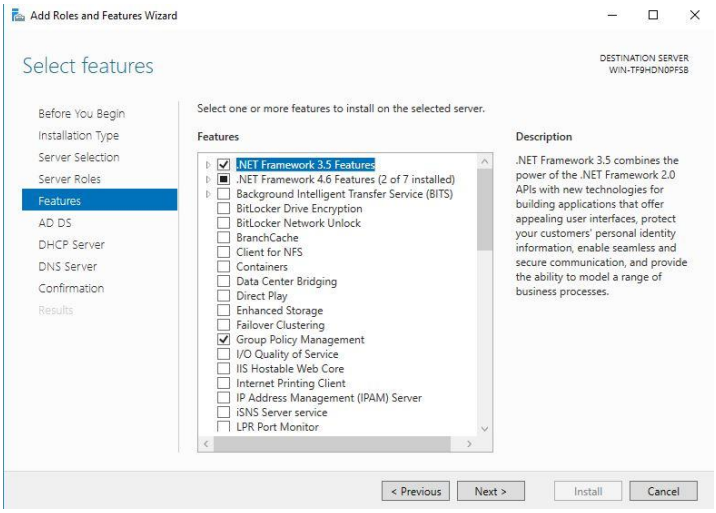


Slika 4.5. – odabir uloga servera

Kao što možemo primijetiti dostupno je još puno uloga koje nismo odabrali. Neke od njih su kratko pojašnjene ispod:

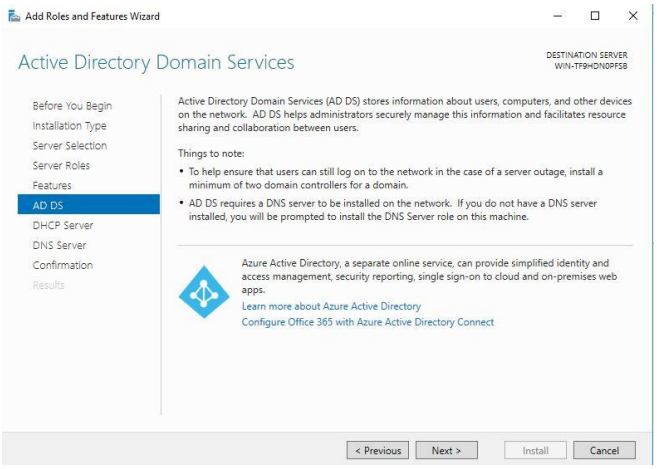
- *Hyper-V* – omogućuje *hosting* i instalaciju te pokretanje virtualnih mašina na serveru (uključujući Windows i ne-Windows mašine).
- *Network Policy and Access Services* – omogućuje RADIUS (*Remote Authentication Dial In User Service*) autentifikaciju. RADIUS je mrežni protokol koji omogućuje autentifikaciju i autorizaciju za uređaje koji se spajaju na mrežu i trebaju koristiti neki dio mreže. Ili drugim riječima, u ovakvom okruženju omogućuje autentifikaciju domenskim računom za druge uređaje koji nisu računala.
- *Print Services* – omogućuje dijeljenje printera. Printeri su instalirani na serveru i svi se poslovi odrađuju na serveru, a klijent samo šalje zahtjev.
- *Web Server* – omogućuje hosting web stranice.
- *Windows Deployment Services* – omogućuje instalaciju Windows OS-a preko mreže koristeći PXE *boot*.
- *Windows Server Update Services* (WSUS) – omogućuje administratorima da odrede koja će ažuriranja za Microsoftove proizvode biti instalirana i kada. Umjesto da svaki klijent preuzima ažuriranje direktno s Microsoftovog servera, ažuriranje se preuzima na WSUS server te klijenti preuzimaju ažuriranje s njega u određeno vrijeme. [7]

Kada su odabrane uloge koje želimo instalirati na server, pritiskom na next dolazimo do idućeg koraka, gdje je potrebno odabrati značajke servera (Slika 4.6.). Značajke su neovisne o ulozi servera i mogu se instalirati na većinu uloga. Možemo ih shvatiti kao neovisne programe koji proširuju mogućnosti sustava.

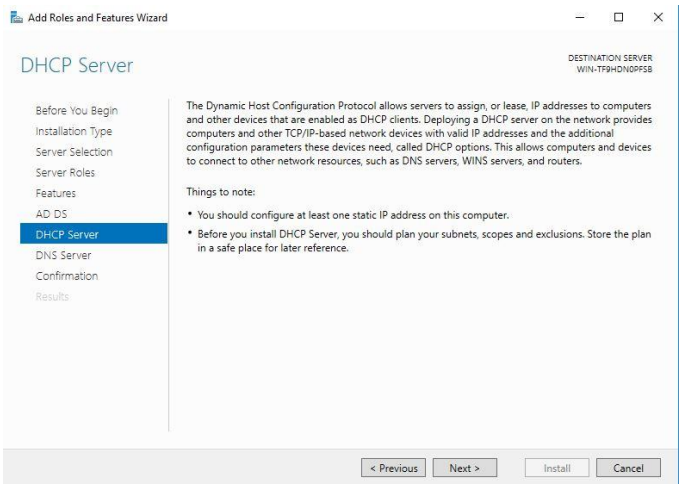


Slika 4.6. – odabir značajki servera

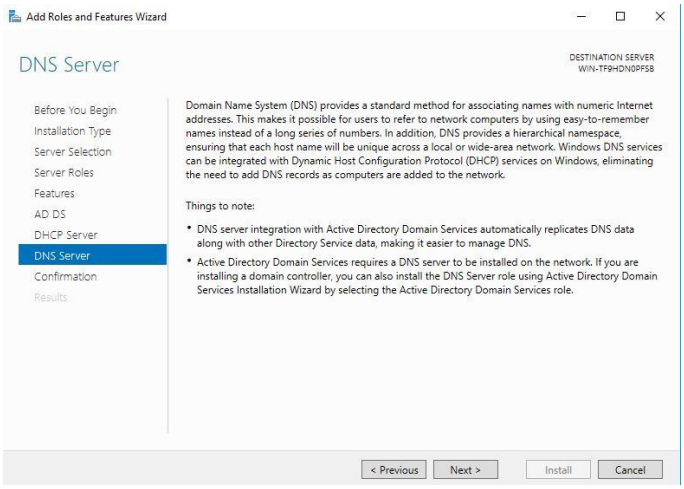
Slijedeća tri koraka su kratki opis svake serverske uloge koje su već objašnjene u prethodnom tekstu (AD DS, DHCP i DNS) (Slike 4.7., 4.8. i 4.9.):



Slika 4.7. – opis AD DS uloge

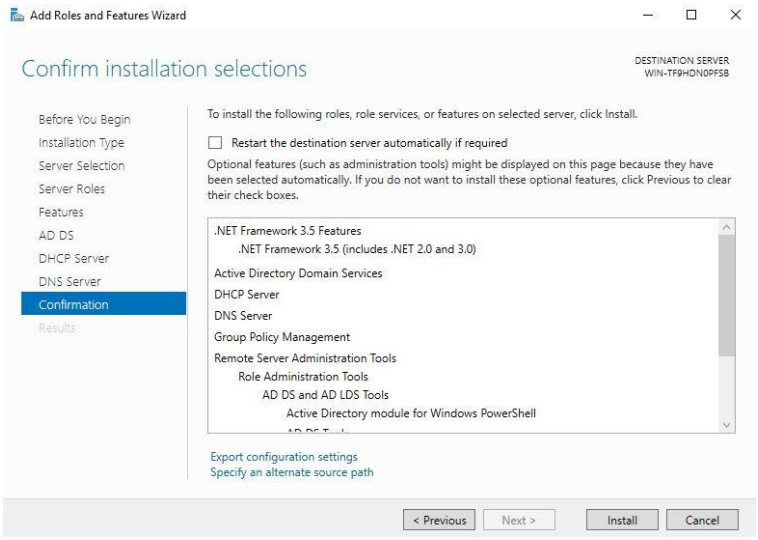


Slika 4.8. – opis DHCP uloge



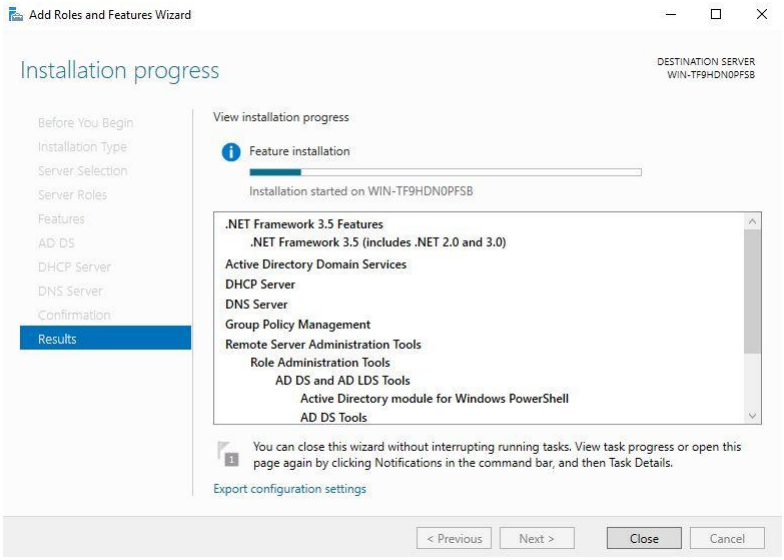
Slika 4.9. – opis DNS uloge

Na sljedećem koraku je dostupan pregled svih odabranih opcija (Slika 4.10.). Ako je sve u redu, kliknemo na *install*:



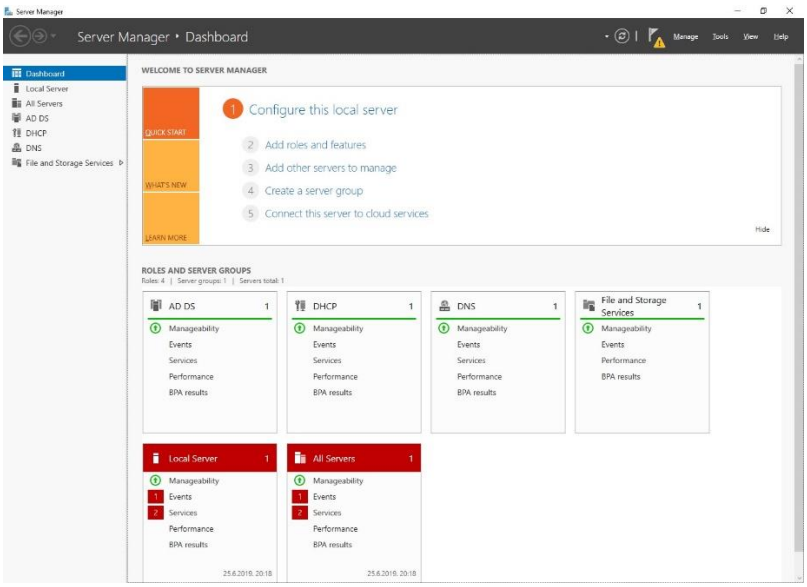
Slika 4.10. – pregled odabranih opcija

Klikom na *install* započinje instalacija odabranih opcija (Slika 4.11). Instalacija može potrajati neko vrijeme, ovisno o broju odabranih opcija i *hardwareskoj* konfiguraciji servera.



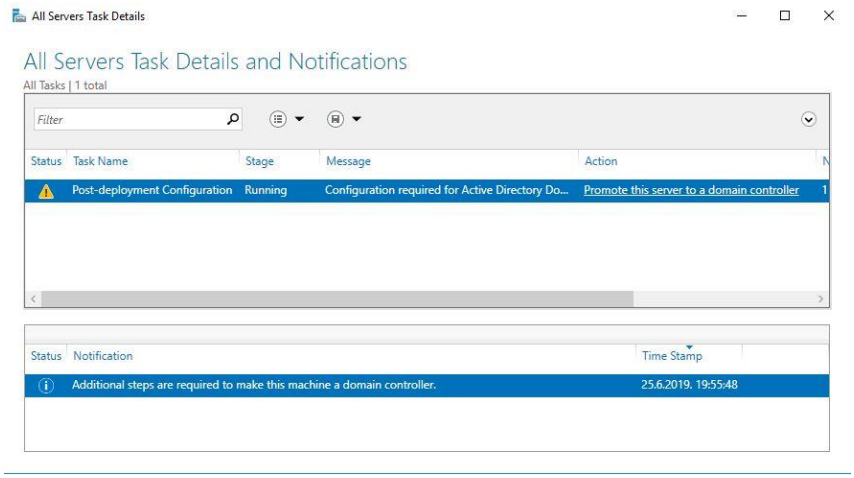
Slika 4.11. – prikaz toka instalacije

Nakon završetka instalacije ponovno se otvara početni zaslon *server managera*, ali sada na njemu možemo vidjeti dodane uloge (Slika 4.12.):



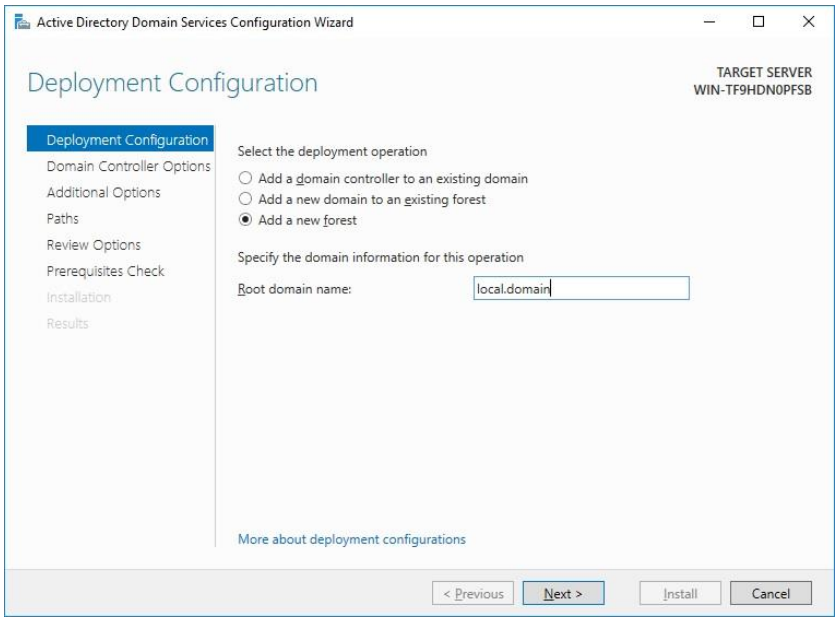
Slika 4.12. – Server Manager nakon instalacije uloga

Ali ovdje posao konfiguracije servera još nije gotov, odnosno još nemamo domenski sustav. Poslije instalacije je potrebna dodatna konfiguracija, odnosno trebamo „promovirati“ server u *domain controller* (Slika 4.13.):



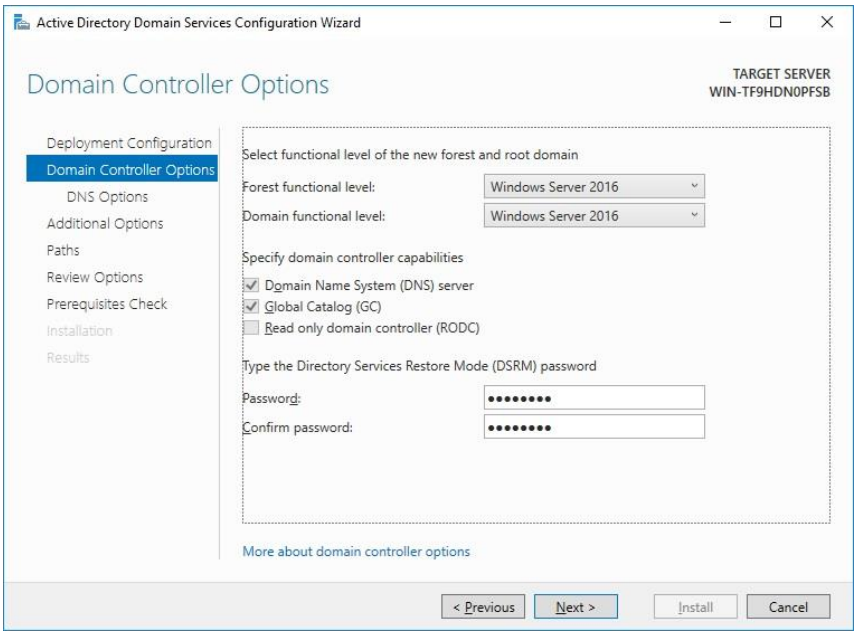
Slika 4.13. – „promoviranje“ servera u domain controller

Sam proces promoviranja servera je automatski i vrlo jednostavan. Potrebno je samo kliknuti na poveznicu Promote this server to a domain controller i pričekati neko vrijeme. Nakon toga vrijeme je za osnovne postavke domene. Pošto nema postojeće infrastrukture odabiremo *Add a new forest* i dajemo ime domeni, u ovom slučaju local.domain. (Slika 4.14.):



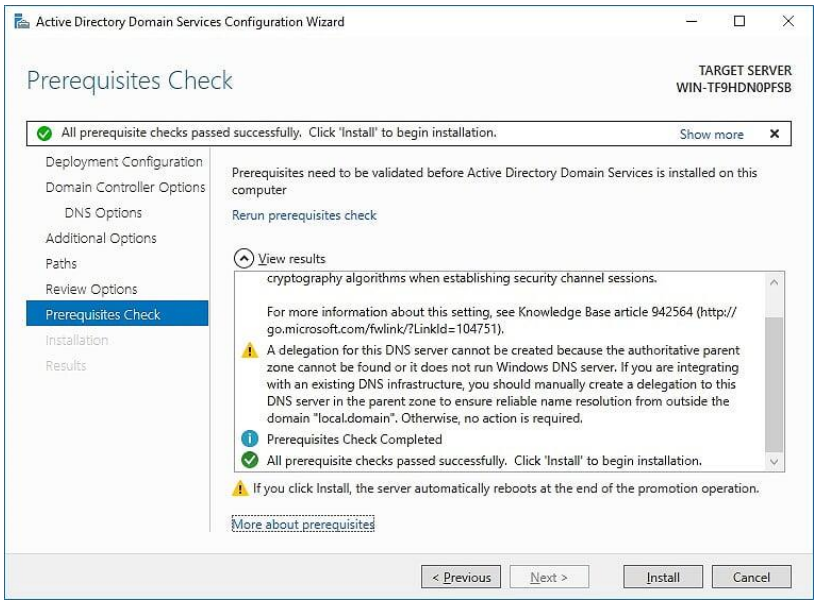
Slika 4.14. – osnovna konfiguracija domene

Klikom na next dolazimo do postavki *domain controllera* (Slika 4.15.), gdje sve ostavljamo na zadanim postavkama te samo dodajemo lozinku za DSRM (*Directory Services Restore Mode*). DSRM možemo najlakše opisati kao *safe mode* za DC, gdje administrator može popraviti ili obnoviti AD bazu podataka.



Slika 4.15. – postavke Domain Controllera

U idućih nekoliko koraka nije potrebno ništa mijenjati, odnosno dovoljno je pritisnuti *Next* i prihvatiti zadane postavke. Ukoliko smo sve pravilno podesili, na provjeri preduvjeta bi trebali dobiti zelenu kvačicu (Slika 4.16.):



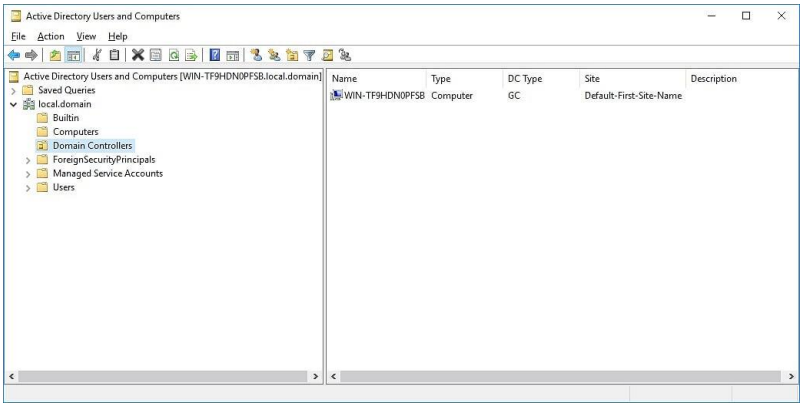
Slika 4.16. – provjera preduvjeta

Ukoliko je sve u redu, možemo kliknuti install i pričekati da se instalacija završi.

Nakon završetka instalacije ponovno nam se otvara početni prozor *server managera* te napokon imamo funkcionalni *domain controller* i možemo uspostaviti domenski sustav. Sada možemo dodavati klijentska računala u domenu, ali prije toga kreirat ćemo domenski račun.

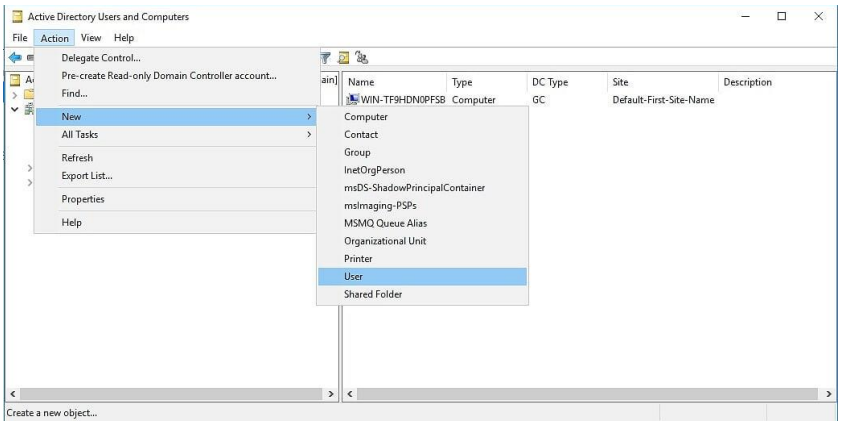
5. DOMENSKI RAČUNI

Da bi kreirali domenski račun prije svega moramo otvoriti *Active Directory*. Do AD-a možemo doći na više načina, preko izbornika Start, Server managera ili ga pak možemo otvoriti upisivanjem komande u *Run* prozor (dsa.msc). Otvara nam se sljedeći prozor (Slika 5.1.):



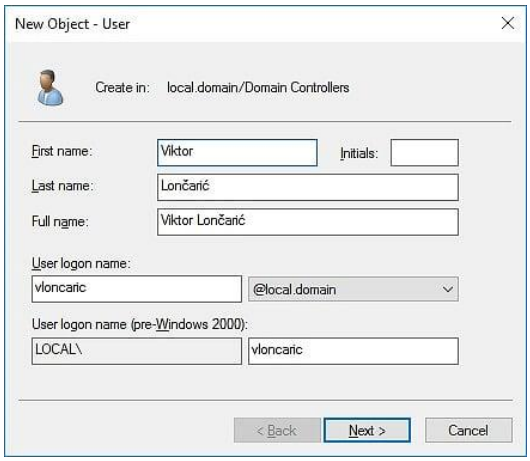
Slika 5.1. – početni prozor AD-a

Novi domenski račun možemo kreirati tako da kliknemo na *Action* izbornik u alatnoj traci, odaberemo *New* i kliknemo na *User* (Slika 5.2.):



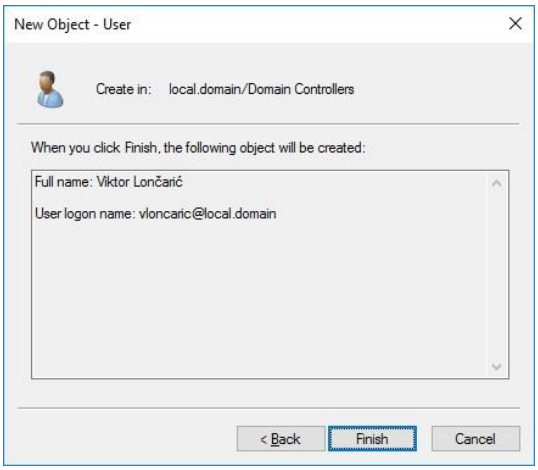
Slika 5.2. – kreiranje domenskog računa

Otvara nam se prozor u koji je potrebno upisati podatke korisnika (Slika 5.3.):



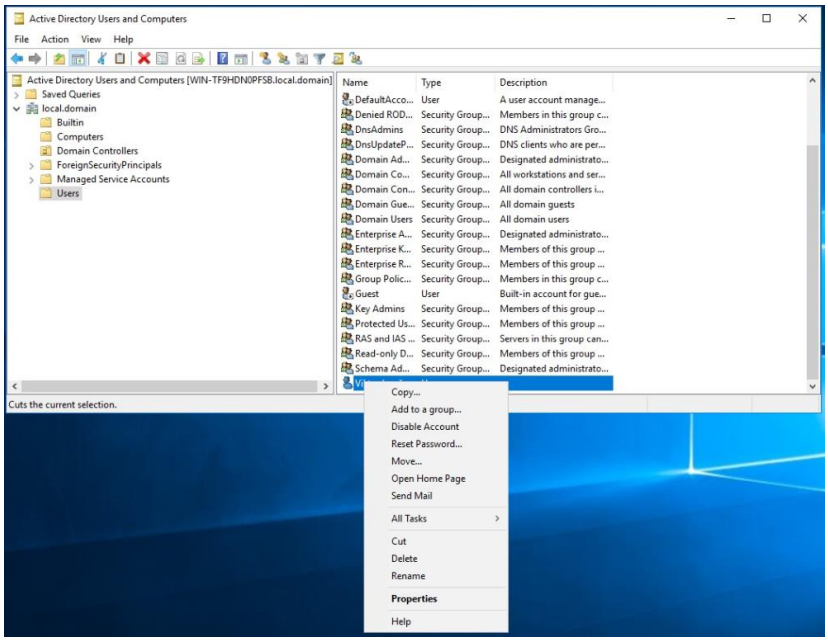
Slika 5.3. – unos korisničkih podataka

Valja istaknuti kako korisničko ime za prijavu kreiramo sami te se ono ne kreira automatski. Klikom na next dolazimo do prozora gdje možemo provjeriti unesene korisničke podatke (Slika 5.4.):



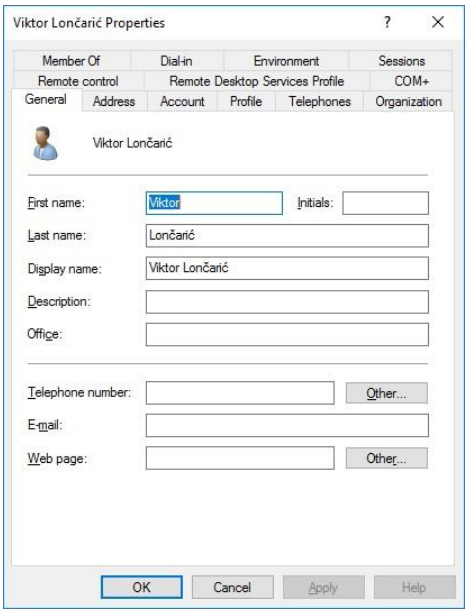
Slika 5.4. - provjera korisničkih podataka

Ukoliko je sve u redu i ne treba ništa promijeniti, kliknemo finish i korisnički račun je kreiran i spremljen je u organizacijsku jedinicu *Users*. Pošto je to trenutno jedni korisnički račun u domeni potrebno mu je dodjeliti administratorska prava na razini domene. To možemo napraviti dodavanjem korisničkog računa u security grupu „*Domain Admins*“. Prije svega potrebno je otvoriti AD sučelje, pronaći željeni korisnički račun (to možemo odraditi „ručno“ ili korištenjem opcije *Find*) te kliknuti desnom tipkom miša na njega te nam se otvara padajući izbornik (Slika 5.5.):[4]



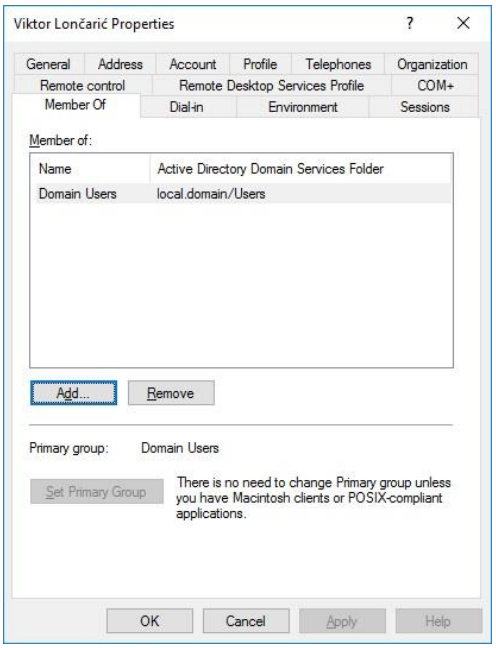
Slika 5.5. – padajući izbornik

Odabiremo properties i otvara nam se prozor sa svojstvima korisničkog računa (Slika 5.6.):



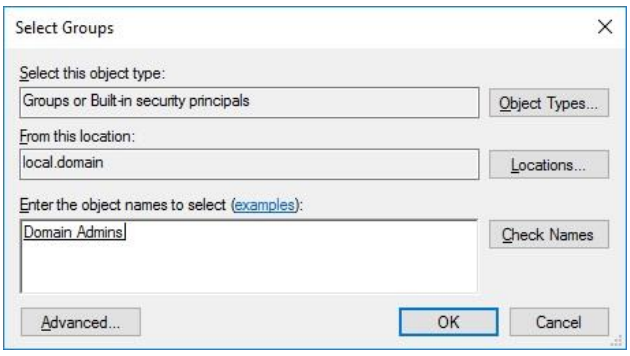
Slika 5.6. – svojstva korisničkog računa

Kao što možemo vidjeti, tu imamo puno mogućnosti. Možemo unijeti dodatne informacije o korisniku (npr. njegovu mail adresu), ali je za naše potrebe potrebno otvoriti *Member Of tab* (Slika 5.7.):



Slika 5.7. – Member of tab

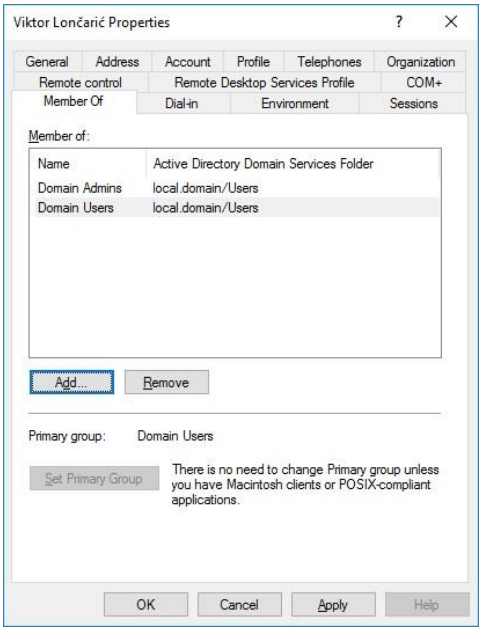
Možemo primijetiti kako je korisnički račun trenutno član samo jedne *security grupe*, *Domain Users*. To je zadana security grupa koja se dodaje svim novim računima. Ukratko, *security grupa* je skup sigurnosnih prava pristupa koja se primjenjuju na korisnički račun. Grupa *Domain Users* ima ograničena prava pristupa, odnosno ne može pristupiti svim dijelovima domenskog sustava. Zato račun dodajemo u *Domain Admins* security grupu i tako omogućujemo puni pristup svim domenskim resursima i upravljanjem istima.[4] Klikom na gumb *Add* otvara nam se zaseban prozor gdje račun možemo dodati u dodatnu *Security grupu*. Za dodavanje je dovoljno početi pisati ime grupe u polje *Object names* i pritisnuti gumb *Check Names*, a sustav će za nas pronaći željenu grupu (Slika 5.8.):



Slika 5.8. – dodavanje security grupe

Moguće je i dodati više grupa odjednom, ali onda je potrebno imena grupa odvojiti zarezima. Kada smo upisali imena željenih grupa izbor je potrebno potvrditi klikom na gumb OK i korisnički račun

je dodan u grupu i sada ima administratorska prava na razini domene. Ako je sve prošlo u redu trebali bi vidjeti *Domain Admins* security grupu u *Member Of tabu* (Slika 5.9.):



Slika 5.9. – Member Of tab nakon dodavanja dodatne Security grupe

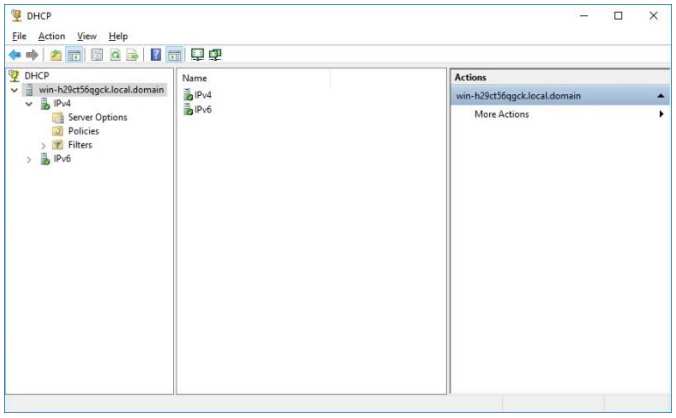
Sada je korisniku omogućen pristup i upravljanje svim dijelovima domene. Korisnik se može svojim domenskim računom prijaviti na server, koristiti *Server manager* i sve njegove alate (npr. AD) bez ikakvih ograničenja.

6. KONFIGURACIJA DHCP SERVERA

Kao što se može primijetiti u prijašnjem tekstu (i slikama) naš server ima i ulogu DHCP servera. Uloga DHCP (*Dynamic Host Configuration Protocol*) servera je već prije objašnjena, a to je dodjeljivanje dinamičkih IP adresa, te takvom ulogom servera izbjegavamo obavezu ručnog dodavanja statičkih IP adresa svakom novom uređaju u mreži. Server će svakom novom uređaju dodijeliti prvu slijedeću slobodnu dinamičku IP adresu iz definiranog opsega. [9]

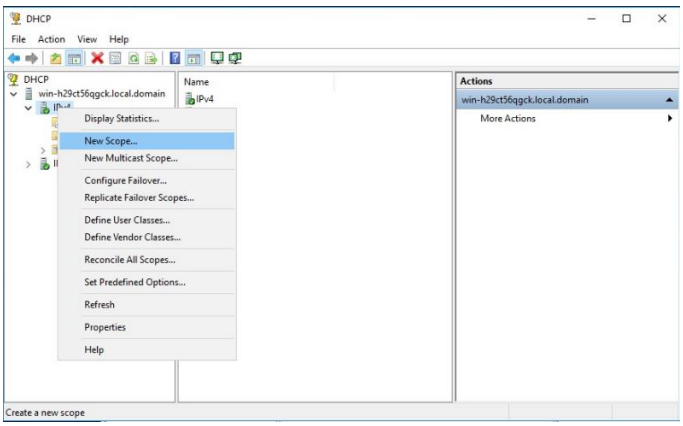
Ali prije svega potrebno je konfigurirati DHCP server.

Prije svega potrebno je doći do postavki DHCP servera, odnosno DHCP uloge našeg servera. U *Server Manageru* kliknemo na *Tools* i odaberemo DHCP. Otvara se slijedeći prozor (Slika 6.1.):



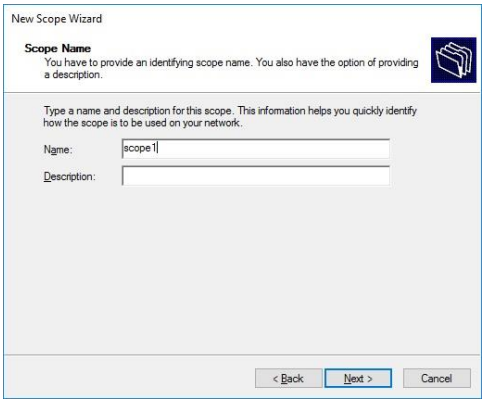
Slika 6.1. – DHCP Prozor

Da bi konfigurirali DHCP server jednostavno je potrebno konfigurirati opseg dinamičkih adresa koje će se dodjeljivati. Da bi to napravili, desnom tipkom miša kliknemo IPv4 i odaberemo *New scope* (Slika 6.2.):



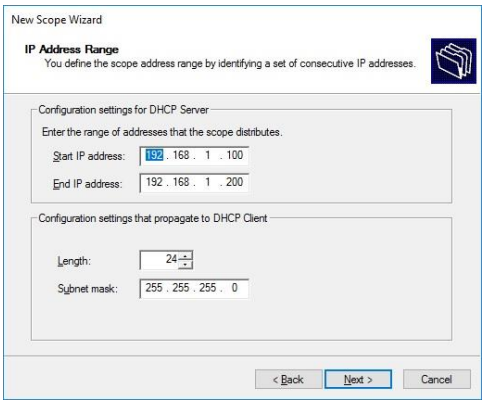
Slika 6.2. – Početak konfiguracije DHCP servera

Nakon toga nam se otvara prozor gdje trebamo dati ime opsegu koji definiramo. Za ovu svrhu će se jednostavno zvati scope1 (Slika 6.3) :



Slika 6.3. – Imenovanje DHCP opsega

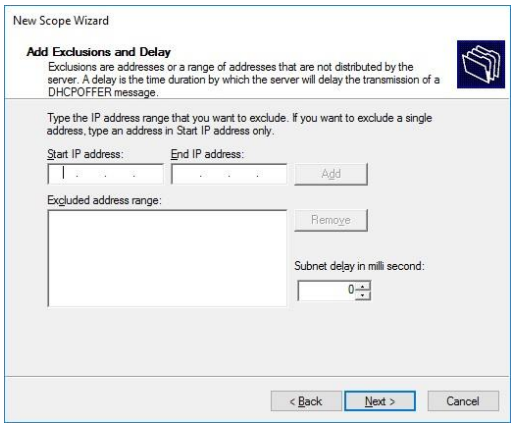
Nakon dodjeljivanja imena vrijeme je da definiramo opseg iz kojeg će se dodjeljivati dinamičke IP adrese. Preporuka je da se za opseg definira jedan dio opsega privatnih IPv4 adresa. Iskoristit ćemo koristiti opseg 192.168.1.100 – 192.168.1.200 (Slika 6.4):



Slika 6.4. – opseg DHCP adresa

Subnet mask se definira automatski.

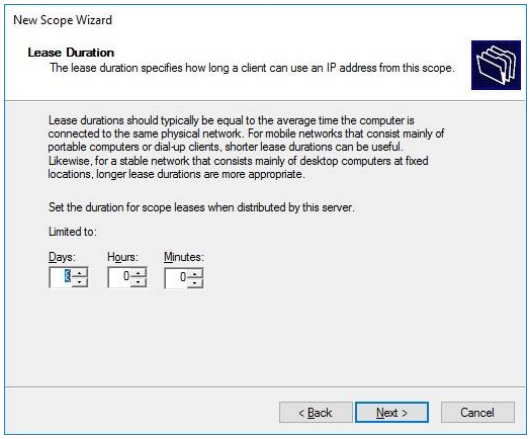
Klikom na next dolazimo do koraka gdje možemo definirati adrese koje želimo isključiti iz opsega, odnosno adrese koje bi inače bile u definiranom opsegu, ali ne želimo da ih server dodjeljuje. U ovom slučaju nema takvih adresa, pa ovo polje ostaje prazno (Slika 6.5.):



Slika 6.5. – Isključive IP adrese

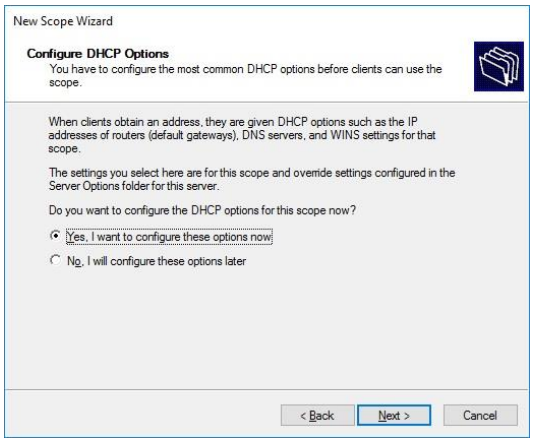
Klikom na Next dolazimo do prozora za odabir trajanja „najma“ IP adrese. Kada istekne „najam“ dinamička IP adresa postaje slobodna i može se dodijeliti nekom drugom uređaju. To je ujedno i glavna razlika između statičke (rezervirane) IP adrese i dinamičke IP adrese.

U ovo slučaju ostaje duljina najma na već zadanoj vrijednosti od 8 dana (Slika 6.6.):



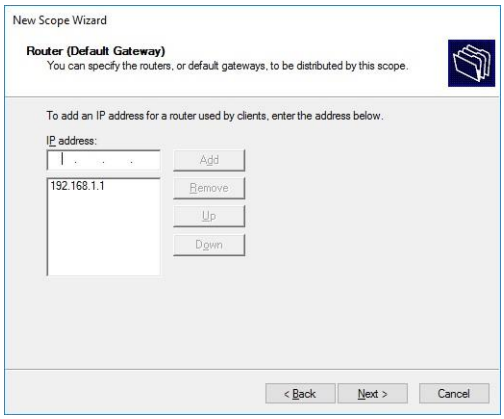
Slika 6.6. – „Najam“ dinamičke IP adrese

Klikom na next dolazimo do upita gdje je potrebno odlučiti želimo li DHCP serveru dozvoliti da definira i druge opcije mreže (DNS, *gateway*, itd.) za zadani opseg. Samo ćemo potvrditi zadanu vrijednost, koja je potvrdan odgovor (Slika 6.7.):



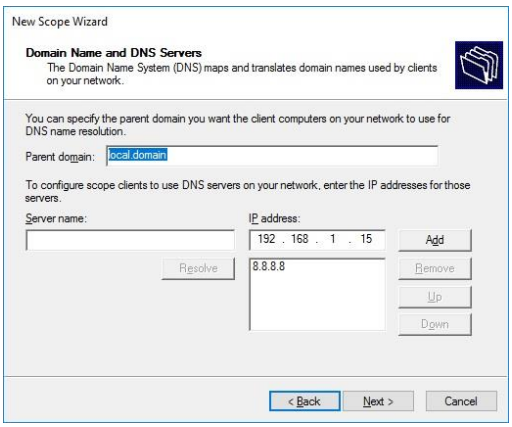
Slika 6.7. – DHCP opcije

Slijedeći korak je definicija *gatewaya*. *Gateway* nije ništa drugo nego *router* u mreži koji nam služi za pristup internetu. U ovoj mreži IP adresa routera je 192.168.1.1 te tu adresu i unosimo i kliknemo na *add* (Slika 6.8.):



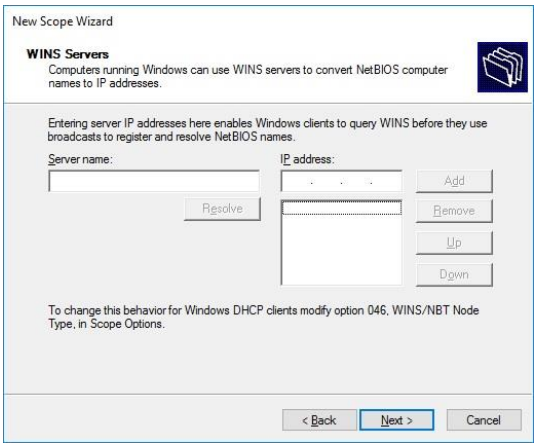
Slika 6.8. – Postavke Gatewaya

Nakon toga potrebno je unijeti adresu DNS servera. Pošto je DNS jedna od uloga našeg servera jednostavno unosimo IP adresu koja odgovara statičkoj adresi servera (Slika 6.9.):



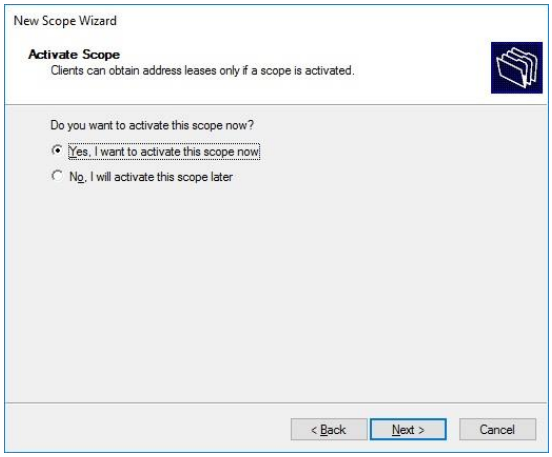
Slika 5.9. – dodavanje DNS servera

Idući korak bi bila definicija WINS servera. WINS (*Windows Internet Name Service*) server služi kao centralno mjesto u mreži na mapiranje *NetBIOS* imena računala i adresa. Uglavnom, funkcija je vrlo slična DNS-u, samo što se ne radi o IP adresama i domenskim imenima. Pošto ovu komponentu ne koristimo, prozor ostaje prazan (Slika 6.10.):



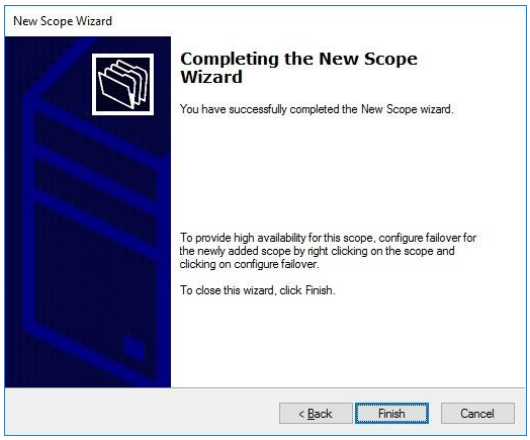
Slika 6.10. – dodavanje WINS servera

U predzadnjem koraku potrebno je klikom na Next potvrditi aktivaciju ovog DHCP opsega (Slika 6.11.):



Slika 6.11. – Potvrda aktivacije DHCP opsega

Klikom na Finish završava konfiguracija DHCP servera te sada svi novi uređaji koji se spajaju na mrežu automatski dobivaju dinamičku IP adresu iz zadanog opsega (Slika 6.12.): [10]

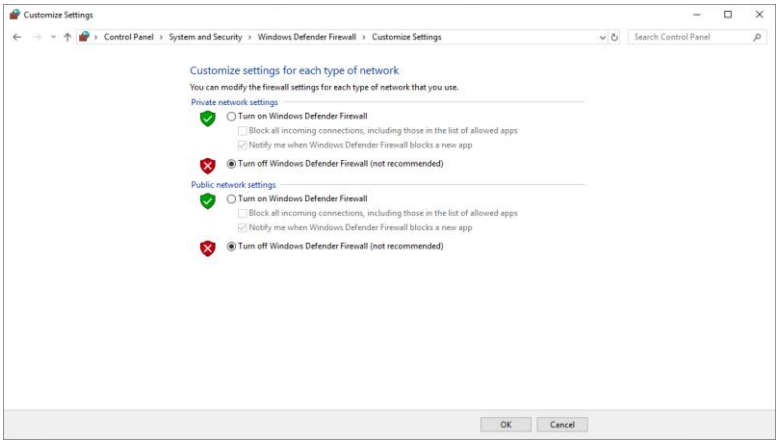


Slika 6.12. – završetak konfiguracije

7. DODAVANJE KLIJENTSKOG RAČUNALA U DOMENSKI SUSTAV

Jedino što još preostaje je dodati klijentsko računalo u domenu. To je kratak i jednostavan proces za koji moraju biti ispunjeni određeni uvjeti. Prije svega, klijentsko računalo i DC moraju biti spojeni u istu mrežu i moraju moći međusobno komunicirati. U našem slučaju na klijentsko računalo instaliran je Windows 10 Pro 64 bit ver. 1903 OS.

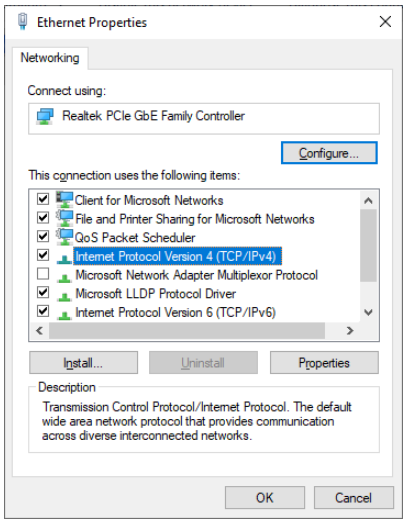
Prije svega potrebno je isključiti *Windows Firewall* iz *Control Panela* (*Control Panel* > *System and Security* > *Windows Firewall* > *Turn Windows Firewall on or off*). Važno je napomenuti kako su za ovaj korak potrebna administratorska prava, kako na serveru tako i na klijentskom računalu (Slika 7.1.):



Slika 7.1. – Windows Firewall

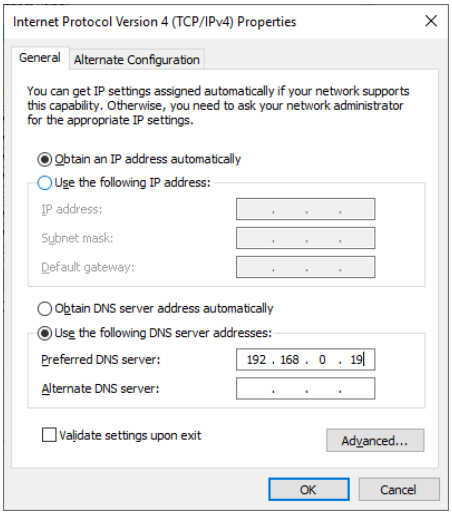
Postupak je identičan na klijentu i na serveru.

Nakon isključivanja *firewalla*, potrebno je na klijentu postaviti mrežne postavke. Primarni DNS server treba biti postavljen na statičku adresu koja će biti adresa IP DC-a. Mrežne postavke također možemo pronaći u *Control Panelu*, pod *Network and Internet*, gdje otvaramo *Network and Sharing Center* te kliknemo na *Change adapter settings* s desne strane. Otvara se prozor gdje možemo vidjeti sve instalirane mrežne adaptere (fizičke i virtualne). Odabiremo adapter preko kojega smo umrežili klijent s DC-om, kliknemo na njega desnom tipkom miša i odaberemo *Properties*. Potrebno je podesiti postavke IPv4 protokola kojeg koristi adapter, pa s liste odabiremo IPv4 i kliknemo properties (Slika 7.2.):



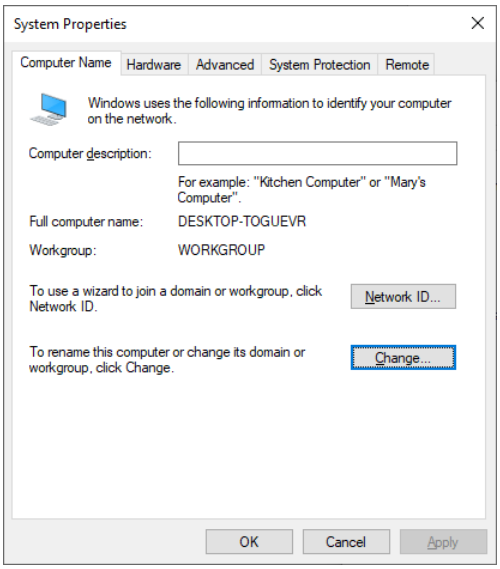
Slika 7.2. – postavke adaptera

Sada je potrebno je podesiti adresu na klijentu na IP adresu našeg DNS servera, odnosno na IP adresu DC-a. U ovom slučaju to izgleda ovako (Slika 7.3.):



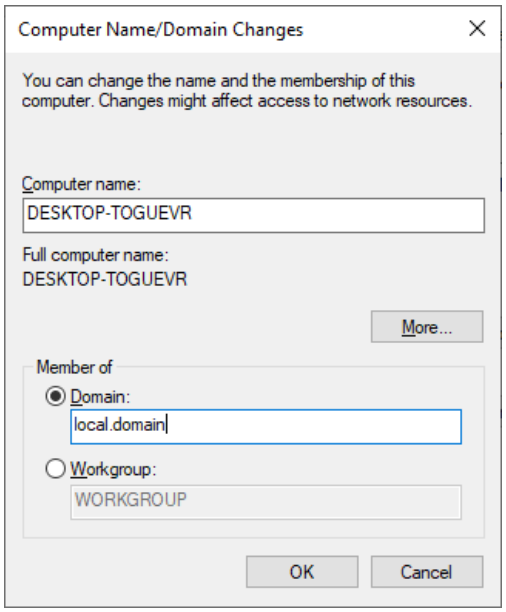
Slika 7.3. – DNS postavke

Klikom na OK ispunjeni su svi preduvjeti za dodavanje klijentskog računala u domenu. Kako bi to napravili otvaramo *This PC*, klikamo na prazan prostor i otvaramo properties. Kada nam se otvori prozor s svojstvima računala pod *Computer name, domain and Workgroup settings* kliknemo na *Change settings*, te nam se otvara slijedeći prozor (Slika 7.4.):



Slika 7.4. – System properties

Da bi dodali računalo u domenu pritišćemo gumb *Change*, te nam se otvara prozor gdje možemo promijeniti ime računala ali i dodati računalo u domenu (ili u *Workgroupu*). Prije svega pod *Member of* je potrebno odabrati opciju da će računalo biti član domene, a potom upisujemo i ime domene. U ovom slučaju to izgleda ovako (Slika 7.5.):



Slika 7.5. – dodavanje klijenta u domenu

Klikom na OK potrđujemo da računalo želimo dodati u domenu. Ako je sve u redu, ako klijent i DC mogu međusobno komunicirati na zaslonu se prikazuje prozor u koji treba unijeti podatke za prijavu domenskog administratora. Ukoliko su podaci za prijavu točni, na zaslonu izlazi dialog box koji nas obavještava da smo uspješno dodali računalo u domenu.

8. GROUP POLICY

Sada kada smo dodali računalo u domenu i kreirali korisnički račun možemo definirati *Group Polic*y pravila. U daljnjem tekstu su navedene neke on najčešće korištenih funkcionalnosti.

Group Policy je još jedna od brojnih domenskih funkcionalnosti. Može biti izrazito korisna kada treba administrirati veliki broj računala, zato što nam omogućuje podešavanje lokalnih postavki klijenta sa servera. GP pravilo definiramo stvaranjem *Group Policy* objekata (GPO). GPO nije ništa drugo nego skup konfiguracija koje se primjenjuju na klijenta. Pomoću GP-a možemo konfigurirati veliki broj postavki. Navedene su neke najčešće mogućnosti:

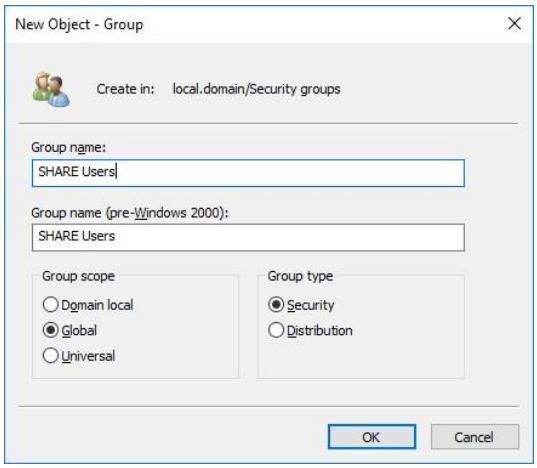
- REDIREKCIJA MAPA: Uzmimo slučaj da tvrtka želi da svi zaposlenici spremaju svoje podatke na lokaciju na serveru. Zadana lokacija za spremanje dokumenata je *C:\Users\(Username)\Documents*. Pomoću GP-a možemo definirati da se sve datoteke koje korisnik naočigled sprema u *Documents* mapu automatski spremaju u određenu mapu na nekoj lokaciji na serveru. U većini slučajeva korisnik neće ni primjetiti razliku, zato što će klikom na svoju *Documents* mapu zapravo pristupati udaljenoj mrežnoj lokaciji, a ne lokalnoj mapi.
- PROMJENA POSTAVKI RAČUNALA: GP možemo iskoristiti i za promjenu postavki računala. Uzmimo za primjer *Power Options* u *Control Panelu*. Pomoću GP-a je moguće definirati da se svi monitori ugase nakon 15 minuta neaktivnosti. Možemo uzeti i za primjer promjenu zadane pozadine radne površine. Valja napomenuti kako je također moguće „zaključati“ korisniku promjenu postavki.
- SIGURNOSNE POSTAVKE: Pomoću GP-a je moguće i definirati razne sigurnosne postavke. Iz prijašnjeg dijela teksta možemo zaključiti kako je u *Control Panelu* moguće definirati želimo li da *Windows Firewall* bude uključen ili isključen. Osim toga moguće je definirati i druge sigurnosne postavke, kao duljinu i kompleksnost lozinke. Isto tako je moguće „zaključati“ korisnički račun ako korisnik previše puta pogriješi pri unosu svojih podataka za prijavu.
- MAPIRANJE MREŽNIH LOKACIJA I PISAČA: GP možemo iskoristiti i za automatsko mapiranje dijeljenih mrežnih diskova (i mapa) na korisničko lokalno računalo. Za primjer pretpostavljamo kako tvrtka na svom file serveru ima zajedničku djeljenu mapu, kojoj mogu pristupiti svi korisnici i mjenjati, odnosno dijeliti njen sadržaj. Ta mapa se nalazi na nekoj mrežnoj lokaciji, odnosno na file serveru, i u svrhu ovog primjera neka njena putanja

bude *\\FS\Mapa*. Koristeći GP možemo automatski mapirati ovu mapu svakom korisniku koji njoj treba imati pristup, te će mu se ista pojaviti u *This PC* sistemskoj mapi kao mrežna lokacija. Slična je sitacija i s pisačima. Ukoliko u domenskom sustavu postoji *Print Server* i na njemu postoji instalirani pisač, taj pisač možemo automatski instalirati na lokalna računala.

U ovom radu ćemo za primjer uzeti mapiranje dijeljene mape pomoću GP-a.

Prije svega je potrebno kreirati mapu koju ćemo podijeliti s drugim korisnicima. To je najjednostavnije napraviti na C particiji diska na našem DC-u. Jednostavno pomoću *Windows Explorera* uđemo u C: direktorij, kliknemo desnom tipkom miša na prazni prostor i odaberemo *New* > *Folder*. Mapu nazovimo jednostavno „share“.

Idući korak je kreiranje *Security grupe* u AD-u u koju ćemo staviti korisnike koji će imati pristup mapi. To možemo napraviti tako da kliknemo desnom tipkom miša na Organizacijsku jedinicu u kojoj želimo stvoriti novu *Security grupu*. Zatim je potrebno odabrati *New* > *Group*. Otvara nam se prozor u koji je potrebno upisati ime grupe i odabrati vrstu grupe (Slika 8.1.):



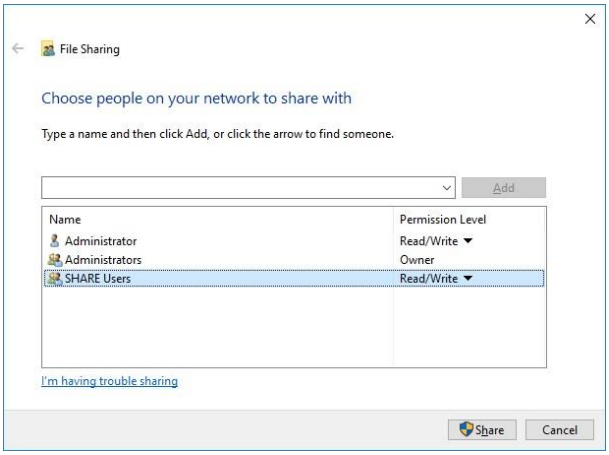
Slika 8.1. – Kreiranje nove Security Grupe

U našem slučaju grupa će se zvati SHARE Users, a tip grupe naravno ostaje *Security*. *Group Scope* možemo ostaviti na zadanoj postavci. Klikom na OK kreiramo novu *Security grupu*.

Sada je potrebno željene korisnike dodati u novu grupu. Postupak je identičan kao dodavanje u grupu Administrators, a jedina je razlika ime grupe.

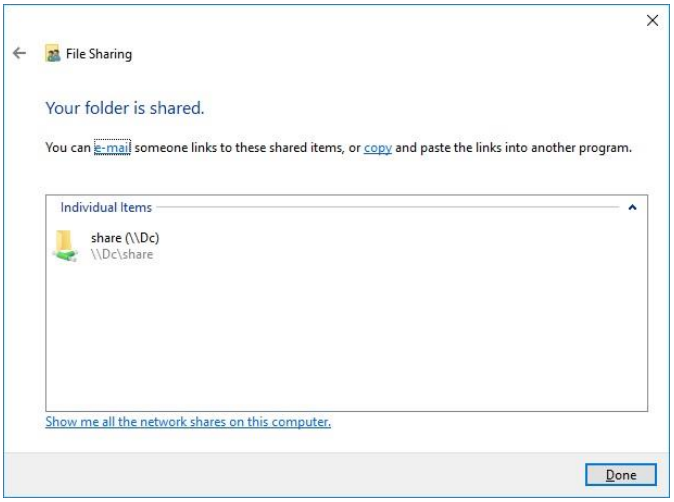
Nakon toga trebamo podijeliti mapu korisnicima koji su članovi grupe. Kliknemo desnom tipkom miša na mapu, odaberemo *Properties* i otvorimo Sharing tab. Tu možemo vidjeti kako naša mapa nije podijeljena nikome po tome što nema mrežnu putanju. Klikom na tipku Share otvara se prozor

u kojem je potrebno odabrati s kime ćemo podijeliti mapu. Možemo upisati ime naše security grupe (SHARE Users) i kliknuti na gumb *Add* (Slika 8.2.):



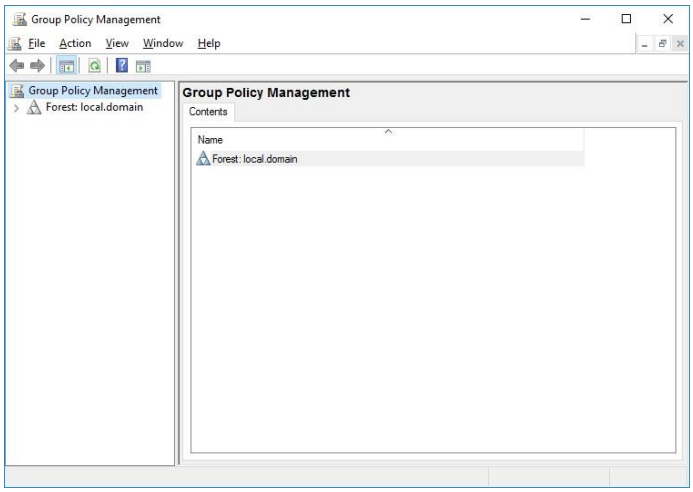
Slika 8.2. – dijeljenje mape

Klikom na *Share* dodjeljujemo pristup mapi svim korisnicima koji su članovi *Security grupe*, te se prikazuje prozor (Slika 8.3.) koji to potvrđuje i u kojem možemo pročitati mrežnu putanju mape (u ovom slučaju je to \\Dc\Share):



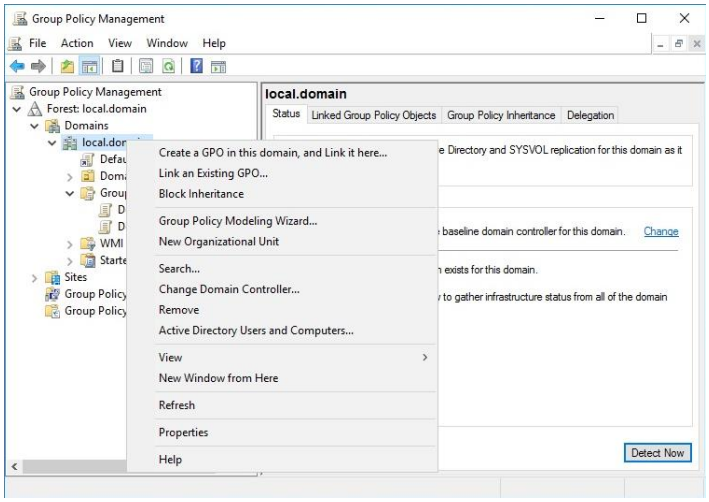
Slika 8.3. – potvrda dijeljenja mape

Sada korisnici s kojima smo podijelili mapu mogu pristupiti mapi i njenom sadržaju pomoću mrežne putanje. Iako se čini jednostavno taj način pristupa je i dalje nezgodan za prosječnog korisnika. Iz tog razloga želimo automatski mapirati mapu korisnicima koji imaju pristup, odnosno članovima *Security grupe* SHARE Users. Tu ćemo se poslužiti jednom od mogućnosti GP-a. Prije svega je potrebno otvoriti *Group Policy Management* konzolu. Možemo je pronaći u *Start menu* u *Administrative tools* mapi. Početni prozor izgleda ovako (Slika 8.4.):



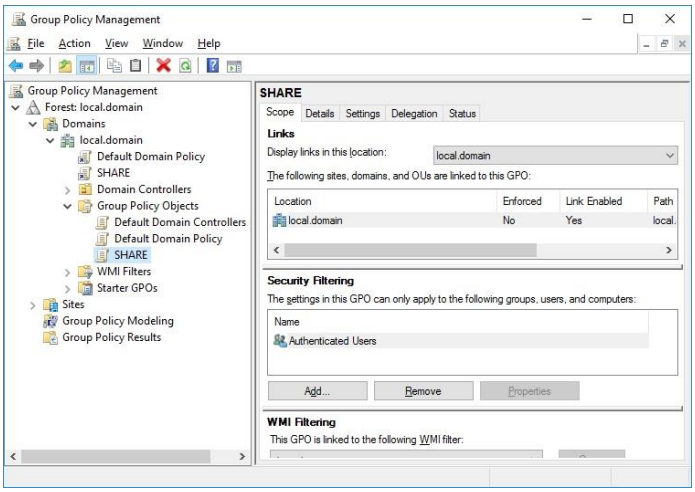
Slika 8.4. – Group Policy Management konzola

Potrebno je raširiti forest na lijevoj strani kako bi došli do naše domene. Kada smo proširili forest i vidimo domenu kliknemo desnom tipkom miša na domenu i odaberemo *Create a GPO in this domain, and Link it here…* (Slika 8.5.):



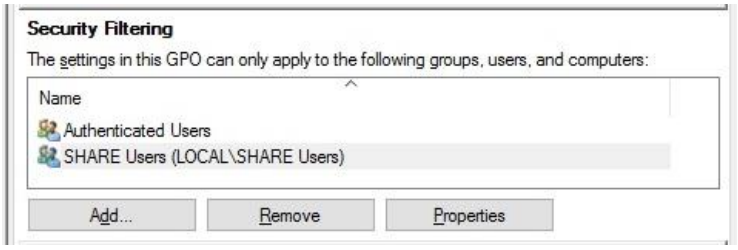
Slika 8.5. – kreiranje novog GPO

Nakon toga nam se otvara prozor u kojem je potrebno imenovati novi GPO. U našem slučaju zvat će se jednostavno SHARE. Kada potvrdimo ime možemo vidjeti novi GPO u hjerarhijskoj strukturi s lijeve strane, u OU *Group Policy Objects* (Slika 8.6.):



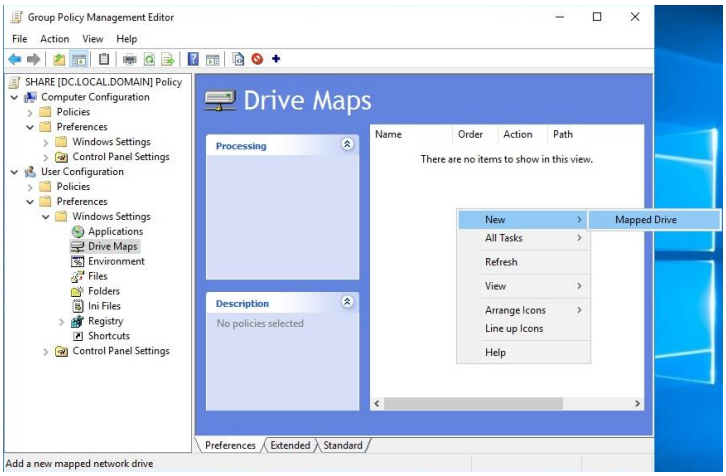
Slika 8.6. – Prikaz novog GPO

Nakon toga je potrebno definirati na koga će se primjenjivati taj GPO. To možemo napraviti klikom na gumb ADD pod *Security Filtering*, gdje nam se pojavljuje prozor u koji upišemo ime naše *Security grupe*. Kada potvrdimo odabir, u dijelu prozora *Group Policy Management* pod *Security Filtering* bi trebali vidjeti našu *Security grupu*, što znači da će se ovaj GP primjenjivati na sve grupe (ili ostale objekte) koji se tu nalaze (Slika 8.7.):



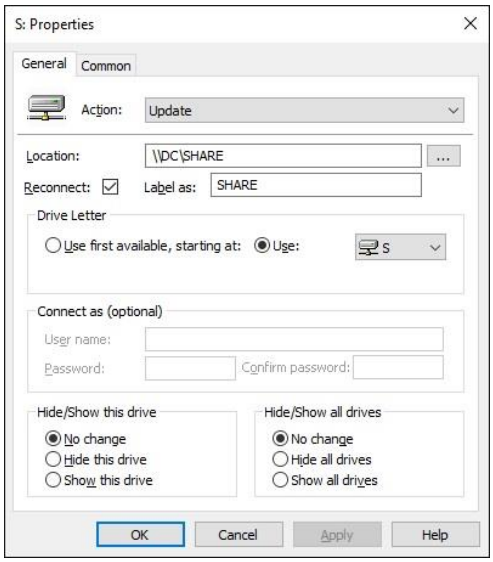
Slika 8.7. – Security Filtering

Sada kada je definirano na koga se GPO primjenjuje potrebno je definirati i samu funkciju GPO. To možemo napraviti tako da kliknemo desnom tipkom miša na naš GPO u hijerarhijskoj strukturi i odaberemo *Edit*, nakon čega nam se otvara GP Editor, gdje možemo definirati funkciju GPO. U našem slučaju odabiremo *Drive Maps*, pod *User Configuration* > *Windows settings*. Sada možemo definirati koji dijeljeni direktorij želimo mapirati i kako. Klikom desnom tipkom miša na prazan prostor odabiremo *New* > *Mapped drive* (Slika 8.8.):



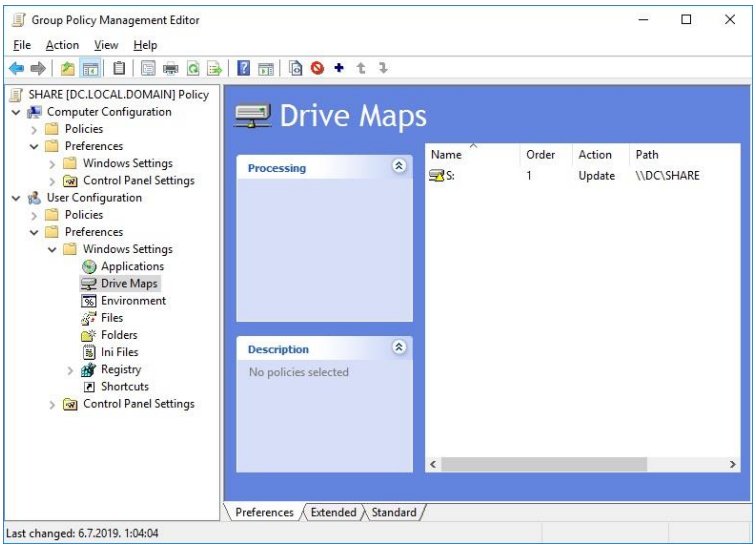
Slika 8.8. – Mapiranje novog dijeljenog direktorija

Otvara se novi prozor u koji je potrebno upisati podatke direktorija koji želimo mapirati (Slika 8.9.):



Slika 8.9. – podaci mapiranog direktorija

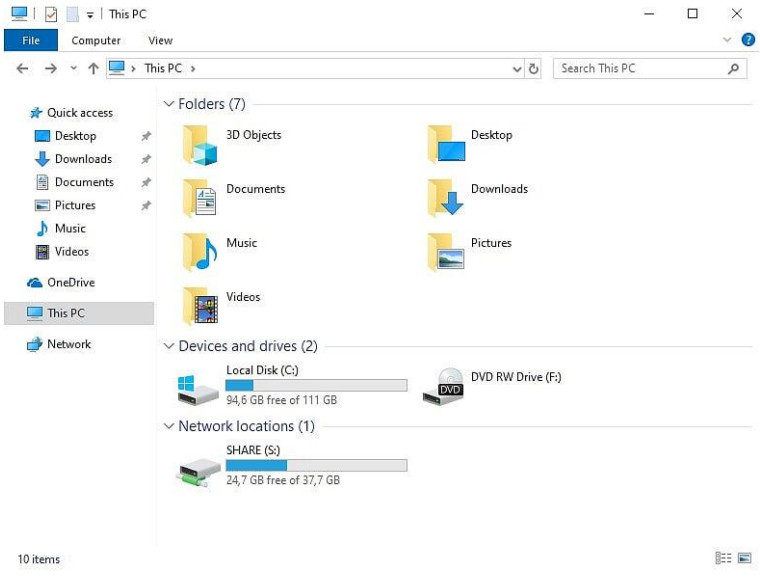
Pod *Location* je potrebno upisati mrežnu putanju dijeljene mape, koju smo dobili kada smo podjelili mapu sa *Security grupom*. Klikom na *checkbox Reconnect* potvrđujemo da želimo da se lokalno računalo svaki puta ponovno spoji s dijeljenim direktorijem kada se korisnik prijavi s svojim računom. *Label as* označava ime koje će dijeljeni direktorij dobiti na lokalnom računalu. Na kraju je potrebno odrediti koje će slovo dobiti mapirani direktorij. Odabrano je slovo S zato što je dovoljno daleko u abecedi i neće biti zauzeto na lokalnom računalu od strane nekih prijenosnih medija, particija ili drugih mapiranih direktorija. Klikom na OK pojavljuje se dijeljeni direktorij u *Drive Maps* popisu (Slika 8.10.):



Slika 8.10. – Drive Maps nakon mapiranja dijeljenog direktorija

Ovime smo završili proces kreiranja GPO za mapiranje dijeljenog direktorija. Uspješno smo kreirali GPO koji se sada primjenjuje na sve korisnike koji su članovi *Security grupe* „SHARE Users“. Sada nam se jedino preostaje prijaviti na klijentsko računalo s računom koji je član grupe i provjeriti primjenjuje li se stvarno GPO i fukncionira li kako je zamišljeno.

Nakon prijave na klijentsko računalo otvaramo *This PC* te pod *Network Locations* možemo vidjeti SHARE (S:) (Slika 8.11.):



Slika 8.11. – This PC mapa klijentskog računala nakon primjene GPO

To znači da se na klijentsko računalo uspješno primjenio GPO i radi kako je zamišljeno.

Ovime je zaključeno poglavlje o *Group Policy*-u. Ovim primjerom je samo zagrebena površina. Mogućnosti GP-a su stvarno raznolike te njegove primjene nisu ograničene na mogućnosti spomenute u ovom radu. [11][12][13]

9. ZAKLJUČAK

Ovim radom obrađena je problematika administracije velikog broja računala. Opisana metoda se najčešće primjenjuje u poslovnom okruženju, zato što nudi mogućnost kontrole računalnog sustava ljudima na rukovodećim pozicijama. Osim navedenog, postoje još mnoge prednosti. Administratorima je uvelike olakšana administracija korištenjem domenskog sustava. Korisnici se mogu prijaviti na bilo koje računalo koje je dodano u domenski sustav sa svojim domenskim računom i početi s radom. Administratori mogu pomoću *Group policya* ograničiti korisnicima pristup postavkama bitnim za rad sustava, mogu automatski mapirati dijeljene direktorije i pisače na klijentska računala, mogu se postaviti zahtjevi za kompleksnost lozinke, postaviti zadanu pozadinu radne površine (npr. logo tvrtke) i tako dalje. Isto tako, moguće je uspostaviti hijerarhiju pomoću domenskog sustava te primijeniti određena pravila za određenu grupu korisnika. Uzmimo za primjer kako treba dati veće ovlasti ljudima na rukovodećim pozicijama, te se njihova prava pristupa i upravljanja trebaju razlikovati od ostalih radnika – to je vrlo lako ostvariti pomoću *Active Directorya*, Organizacijskih jedinica i *Security grupa*. Također olakšano je dodavanje novih korisnika. Potrebno je samo kreirati novi korisnički račun u *Active Directoryu* umjesto lokalnih korisničkih računa na računalu. Korištenjem *Active Directorya* je olakšano i rješavanje problematičnih situacija, kada korisnik zaboravi lozinku za prijavu te u slučaju takvog problema administrator može u nekoliko klikova korisniku resetirati lozinku.

Osim navedenih prednosti domenskog sustava, koje se najčešće koriste valja zamjetiti i ostale prednosti Windows Servera. Server nam može služiti kao *file* server, odnosno mjesto na kojem će korisnici moći spremati svoje podatke koji su bitni za posao ili neke podatke koje žele podijeliti s drugima. Slično kao što server može služiti kao centralno mjesto na kojem će biti spremljeni podaci, može služiti i kao *print server*, odnosno kao centralno mjesto na kojem će biti instalirani pisači, koje kasnije možemo mapirati na klijente. Prednost toga je da klijentsko računalo ne mora imati direktnu fizičku vezu s pisačem, nego samo klijent i pisač moraju biti u istoj mreži kao i server. Praktično gledano, korisnik može koristiti pisač koji je fizički udaljen od njega, npr. u drugoj prostoriji, te može postojati veći, zajednički pisač za sve korisnike.

Još jedna korisna uloga Windows Servera je *Hyper-V*. *Hyper-V* bi bila mogućnost instalacija virtualnih mašina koje se pokreću na serveru. Korisnik se potom može spojiti na virtualni stroj sa svog klijentskog računala. Tako efikasno korisnik radi na serveru te nije potrebno klijentsko računalo snažnih performansi. Još jedna česta upotreba *Hyper-V* usluge je istaliranje virtualnih

instanci servera i uspostavljanje virtualnih lokalnih mreža između virtualnih mašina. Tako se može uštediti novac zato što za svaki potrebni server ne moramo imati fizički server nego jedan fizički server može izvoditi više virtualnih servera.

Osim toga pomoću Windows servera moguće je i značajno olakšati instalaciju i postavljanje većeg broja računala. Pomoću mogućnosti *Windows Deployment Services* možemo napraviti instalacijsku datoteku u koju možemo uključiti osnovne postavke vezano za klijentska računala, upravljačke programe i neke osnovne aplikacije, a što je najbitnije može sadržavati i instalirana ažuriranja s *Windows update servisa*. Ova mogućnost iskorištava opciju novijih računala i matičnih ploča za *boot* s mreže te računalo učitava instalacijsku datoteku operacijskog sustava sa servera putem mreže.

Još jedna mogućnost Windows servera koja se aktivno koristi je *Windows Server Update Services*, koja omogućuje kontrolu instalacije ažuriranja operacijskog sustava. Instalacija ažuriranja može znatno usporiti rad računala te pomoću ove mogućnosti možemo podesiti vrijeme u koje želimo da se ažuriranje instalira te tako rasteretiti klijentska računala. Isto tako manje opterećujemo mrežu, zato što se ažuriranje jednom preuzme na server te onda klijentska računala instaliraju ažuriranje sa servera, a ne s mreže.

U ovom radu je objašnjena i demonstrirana instalacija i podešavanje jednostavnog domenskog okruženja i najčešće korištenih mogućnosti. Glavna razlika koju bi istaknuo između ovog što prikazanog i pravog, realnog poslovnog sustava je osim broja korisnika ta što su u realnom okruženju *Domain Controlleri* i ostali serveri domenskog sustava najčešće virtualne mašine. Razlog što ovdje nisu korištene virtualne mašine je nedostatak opreme, odnosno fizičkog servera i kompleksnije mrežne opreme. Sustav kakav je prikazan ovdje može funkcionirati i u realnom okruženju, samo s puno manje korisnika nego kada imamo pravi fizički server i odgovarajuću mrežnu opremu.

Sve u svemu može se zaključiti kako upotreba Windows Servera uvelike može olakšati posao administratorima kada se radi o većim računalnim sustavima. Domenski sustav rješava problem administracije korisnika, njihovih računa i prava pristupa, pomoću *Hyper-V* usluge možemo instalirati dodatne servere, na serveru možemo držati backup bitnih podataka te nam može poslužiti kao pomoć pri instalaciji većeg broja računala. Osim toga smanjuje troškove poslovanja zato što eliminira potrebu za dodatnom skupom opremom.

10. LITERATURA

1. Windows Server 2016 Improvements - https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-server-2016-improvements

2. What's New in Windows Server 2016 - https://docs.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2016

3. Get Started with Windows Server 2016 - https://docs.microsoft.com/en-us/windows-server/get-started/server-basics

4. Organizational Units - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc978003(v=technet.10)

5. Active Directory Domain Services - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services

6. Understanding the Active Directory Logical Model - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model

7. Server Roles and Technologies in Windows Server 2012 R2 and Windows Server 2012 - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831669(v=ws.11)

8. DNS Overview - https://docs.microsoft.com/en-us/windows/win32/dns/dns-overview

9. Dynamic Host Configuration Protocol (DHCP) - https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

10. DHCP Server - https://docs.microsoft.com/en-us/iis/web-hosting/installing-infrastructure-components/dhcp-server

11. Group Policy Basics – Part 1: Understanding the Structure of a Group Policy Object - https://blogs.technet.microsoft.com/musings_of_a_technical_tam/2012/02/13/group-policy-basics-part-1-understanding-the-structure-of-a-group-policy-object/

12. Group Policy Basics – Part 2: Understanding Which GPOs to Apply - https://blogs.technet.microsoft.com/musings_of_a_technical_tam/2012/02/15/group-policy-basics-part-2-understanding-which-gpos-to-apply/

13. Group Policy Basics – Part 3: How Clients Process GPOs - https://blogs.technet.microsoft.com/musings_of_a_technical_tam/2012/02/22/group-policy-basics-part-3-how-clients-process-gpos/

14. Shematski prikaz Windows domene - https://pcchip.hr/wp-content/uploads/2018/02/windows-domain-mre%C5%BEe.jpg

11. SAŽETAK

U ovom radu obrađivan je problem administracije velikog broja računala spojenih u lokalnu mrežu korištenjem servera s Windows Server operacijskim sustavom. Prije svega bilo je potrebno instalirati sam operacijski sustav na server, što je vrlo jednostavan proces a ima i grafičko sučelje. Nakon toga smo podesili neke osnovne postavke i server je bio spreman za dodjeljivanje specifičnih uloga i konfiguraciju. Problem ne leži u administraciji samo računala, nego je potrebno administrirati i velik broj korisničkih računa. To će nam uvelike olakšati domenski sustav. Za prvu ulogu servera odabiremo Active Directory Domain Services i pratimo daljnje korake za konfiguraciju. Kada se završio proces osnovne instalacije uloge bilo je potrebno server promovirati u Domain Controller i unijeti ime domene. Kada smo uspostavili domenu potrebno je dodati klijentsko računalo u domenu. Važno je napomenuti kako računalo i server moraju biti spojeni u isto mrežu i moraju moći zajednički međusobno komunicirati. Kada dodamo računalo u domenu možemo se na to računalo prijaviti s domenskim računom kojeg smo prethodno kreirali na serveru u Active Directoryu. Kada unesemo domensko korisničko ime i lozinku na serveru se vrši autentifikacija i ako je sve u redu pri prvoj prijavi se stvara domenski profil na klijentu. Također se primjenjuju i Group Policy pravila ukoliko su definirana. To znači da se automatski mapiraju dijeljeni direktoriji, automatski se postavlja pozadina radne površine i sl.

Samim sustavom smo si uvelike olakšali administraciju većeg računalnog sustava zato što smo u mogućnosti s centralne lokacije (server) upravljati korisničkim računima, možemo automatski konfigurirati osnovne postavke na klijentskim računalima koristeći Group Policy te možemo definirati prava pristupa za korisnike.

KLJUČNE RIJEČI:

- Operacijski sustav (OS)
- Server
- Domena
- *Server manager*
- *Domain Controller* (DC)
- *Active Directory* (AD)
- *Domain Name System* (DNS)
- *Dynamic Host Configuration Protocol* (DHCP)

- *Group Policy* (GP)
- *Group Policy Object* (GPO)

WINDOWS SERVER AND DOMAIN SYSTEM

ABSTRACT

In this paper I've tackled the problem of administrating a large number of computers that are connected to a local network using a server running an instance of Windows Server operating system. First, we need to install the operating system on the physical server itself, which is a pretty straightforward process with a graphical user interface. The next step would be to configure some basic settings and then we can start configuring server roles. Our main focus will be on the Active Directory Domain Services role since we also have the administration of user accounts on our hands. Setting up a domain system will make our administrative tasks a lot easier, since we can administer everything from a central location (the server). To set up a domain system, we need to configure the Active Directory Domain Services role first. Configuring the role itself is simple, we just have to follow the setup wizard steps and if we do everything correctly there shouldn't be any major issues. After that we need to promote the server to a Domain controller. We'll also have a setup wizard guiding us through that. The main step here is to actually give a name to the domain. Now that we have setup a domain system we need to add a client computer to the system. But before doing that we need to make sure that the server and the client are connected to the same local network and that they are able to communicate between each other. When we add the client computer to the domain we'll be able to login to our domain account that we previously created in the Active Directory. When we enter our login credentials the server authenticates the user and if the client and the server can communicate and the credentials are correct, a domain profile is created on the client computer during our first login. The group policy rules, such as mapping of a shared directory or a default desktop wallpaper are applied during our first login as well.

The domain system itself is making our task of administrating a large number of computers much easier, because we now have the ability to mange the computers and the user accounts from a central location (the server). We are now able to configure the basic settings on the local clients and configure access rights for different users as well.

KEY WORDS:

- Operating System (OS)
- Server
- Domain
- Server manager
- Domain Controller (DC)
- Active Directory (AD)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Group Policy (GP)
- Group Policy Object (GPO)

ŽIVOTOPIS

Viktor Lončarić rođen je 12.09.1994. u Našicama, u Republici Hrvatskoj. Osnovnu školu u Našicama upisuje 2001. godine, a istu završava 2009. Nakon završenog osnovnoškolskog obrazovanja upisuje srednju elektrotehničku školu u Srednjoj školi Isidora Kršnjavoga u Našicama. Za vrijeme srednjoškolskog obrazovanja ističe se kao vrlo uspješan učenik koji je sudjelovao na mnogim natjecanjima iz područja elektrotehnike i informatike, te sudjeluje u stvaranju školskog godišnjaka kao tehnički urednik. Stručnu praksu obavlja u lokalnom servisu računala i elektronike, gdje stječe važna iskustva za daljni rad. Za vrijeme srednjoškolskog obrazovanja stječe Microsoftov industrijski certifikat *Windows operating system fundamentals* 2012. godine. Srednjoškolsko obrazovanje, koje je nedvojbeno imalo velik utjecaj na daljni odabir karijere završava 2013. godine i stječe zvanje tehničar za elektroniku. Obrazovanje nastavlja na Elektrotehničkom fakultetu u Osijeku, gdje 2013. upisuje stručni studij informatike. Za vrijeme studija stekao je i razna iskustva izvan fakultetskog okruženja. Godine 2016. se zapošljava kao kućni majstor – elekrotehničar u turističkom postrojenju Istraturist u Umagu, gdje je stekao prva radna iskustva. Na nastavak karijere i odabir budućih poslova velik utjecaj je imala stručna praksa koju je za vrijeme studija obavio u odjelu informatike u Nexe grupi u Našicama. Prvi posao u struci mu je bio pozicija *Windows support tech* u osječkoj podružnici tvrtke Hands on server support, gdje se ne zadržava dugo. Početkom 2019. godine prelazi na radno mjesto Windows System administratora u tvrtku Tipico, u Slavonski Brod, gdje radi i sada.