Implementacija sigurnosnih politika u umreženim sustavima

Knezić, Tomislav

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

VARAŽDIN

Implementacija sigurnosnih politika u umreženim sustavima

ZAVRŠNI RAD

Zabok, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

VARAŽDIN

Tomislav Knezić

Z-36919/08-IZV

Implementacija sigurnosnih politika u umreženim sustavima

ZAVRŠNI RAD

Mentor:

Izv. prof. dr. sc. Magdalenić Ivan

Zabok, 2021.

Sadržaj

1. Uvod

U 21. stoljeću teško je zamisliti uređaj koji nije umrežen. „Umreženo“ znači povezano u jednu cjelinu, tzv. računalnu mrežu u kojoj se mogu razmjenjivati informacije, odnosno dijeliti različiti resursi. Svi se uređaji i računala u računalnoj mreži mogu povezati na Internet. Internet je također računalna mreža, odnosno, kako je zovemo „mreža svih mreža“.

Uz sve pozitivno i sve prednosti koje nudi računalna mreža, olakšanje poslovanja, automatizacija i kontrola, podosta sve to baci u sjenu negativna strana. Ogroman je broj korisnika računala i informacijskih sustava. Dobar dio njih nije dovoljno educiran, za neke se može reći da su i nemarni. Rad za računalom svodi im se na „naštrebane“ radnje ili nešto što im netko savjetuje. To su prepoznali zlonamjerni korisnici te vrlo lako iskoriste takve radnje u svrhu dobivanja podataka o sustavu ili čak zaporke za prijavu.

Administratori, odnosno, stručnjaci za sigurnost uvelike rade na samoj edukaciji korisnika sustava te potaknuti ih na razmišljanje prije samog „klikanja“. Informacijski sustav ne može se u potpunosti zaštititi i to je činjenica koje mora biti svjestan svaki korisnik. Radnje administratora u cilju povećanja sigurnosti sustava vrlo su individualne zbog individualnosti samih informacijskih sustava i stoga se ne mogu definirati univerzalne radnje prema kojima bi se gradila sigurnost sustava. Individualnost je u planiranju sigurnosti i vrlo preporučljiva, jer se na taj način otežava planiranje i izvršavanje napada od strane zlonamjernih korisnika.

Svaki korisnik ima svoju ulogu u poslovanju i svaki korisnik ima drugačija prava i ovlasti. Iz tog razloga potrebno im je pojedinačno dodijeliti ovlasti, prava, korisnička imena, a način dodjeljivanja se vodi putem centraliziranog sustava gdje administrator s jednog poslužitelja može kontrolirati sve korisnike i s glavnog poslužitelja dodjeljivati sva prava i ovlasti korisnika.

U ovom završnom radu govori se o „Implementaciji sigurnosnih politika u umreženim sustavima“, odnosno, računalnoj mreži. Rad se sastoji od pet poglavlja.

Prvo poglavlje je uvod u kojem ćemo dati par uvodnih riječi. U drugom poglavlju dotaknuti ćemo se Windows Servera 2019 te instalacije istog. Treće poglavlje fokusira se na Active Directory, četvrto poglavlje odnosi se na Group policy, odnosno implementaciju sigurnosnih politika. Peto poglavlje je zaključak.

2. Windows Server

2.1 Općenito o Windows serveru

Windows Server je niz operacijskih sustava koje Microsoft posebno stvara za upotrebu na poslužitelju. Poslužitelji su iznimno moćni strojevi koji su dizajnirani da rade neprestano i pružaju resurse za druga računala. To znači da se u gotovo svim slučajevima Windows Server koristi samo u poslovne svrhe.

Microsoft je pod tim imenom objavio Windows Server od pokretanja sustava Windows Server 2003. Međutim, i prije toga bile su dostupne poslužiteljske verzije sustava Windows. Na primjer, Windows NT 4.0 bio je dostupan i na radnoj stanici (za opću upotrebu) i na poslužitelju.

U gotovo svim slučajevima, normalni korisnici ne moraju brinuti o Windows poslužitelju. Nećete ga pronaći na polici u trgovinama ili ga slučajno preuzeti s Microsofta kada namjeravate nabaviti standardnu verziju sustava Windows. No, dobro je znati i za ovu verziju kako biste bili svjesni da postoji.

Samo kratkim pogledom možda ćete imati problema reći razliku između Windows poslužitelja i normalnih verzija sustava Windows. Radna površina izgleda isto, uključujući programsku traku, ikone na radnoj površini i gumb Start.

Kako se pokazalo, svako izdanje sustava Windows Server odgovara potrošačkoj verziji sustava Windows. Windows Server 2003, na primjer, poslužiteljska je verzija Windows XP. Trenutne verzije uključuju Windows Server 2016, koji se temelji na godišnjici ažuriranja za Windows 10, i Windows Server 2019, temeljen na verziji 1809 sustava Windows 10. Windows Server 2019 je i baza ovog završnog rada.

Budući da Windows Server i Windows dijele bazu kodova, na oba možete izvesti mnoge iste funkcije. Na Windows Server možete preuzeti i instalirati programe poput preglednika i uređivača fotografija, a mnoge osnove sustava Windows, poput Notepada, uključene su u Windows Server.

Budući da je Windows Server namijenjen tvrtkama, uključuje obilje poslovnog softvera. Ispod je nekoliko uloga koje poslužitelj može izvesti zahvaljujući ovim alatima:

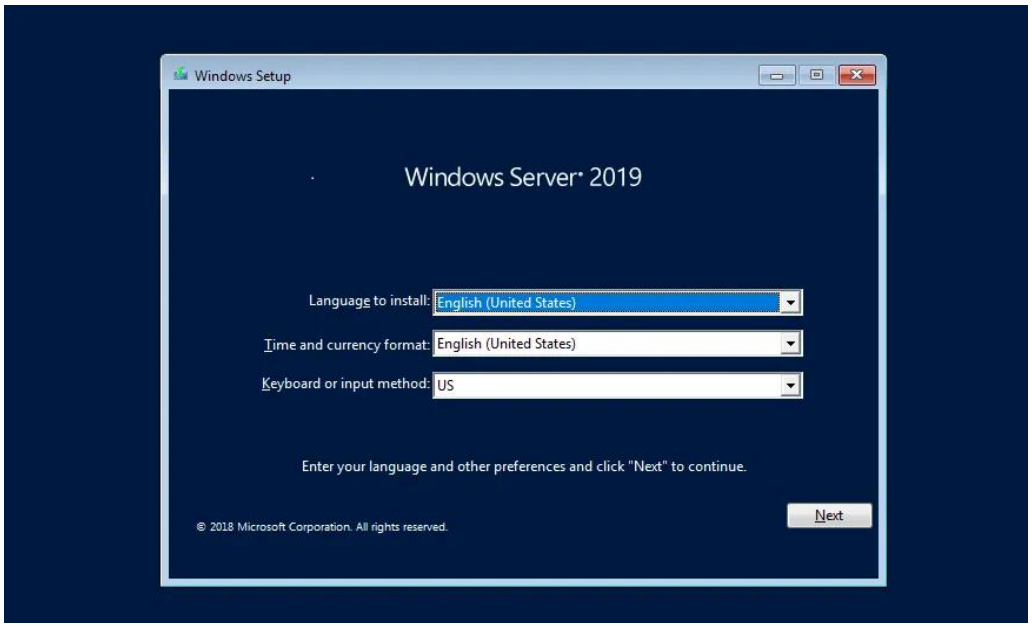
- Active Directory: Active Directory je usluga upravljanja korisnicima koja omogućuje poslužitelju da djeluje kao kontroler domene. Umjesto da se svaki korisnik prijavi na lokalno računalo, kontroler domene upravlja cijelom autentifikacijom korisničkog računa.
- DHCP: Protokol za dinamičku konfiguraciju hosta je protokol koji omogućuje poslužitelju da automatski dodijeli IP adrese svim uređajima na mreži. Kod kuće, vaš usmjerivač to vjerojatno rješava. No, u poslovnom okruženju, IT osoblje može iskoristiti veću DHCP funkcionalnost u Windows poslužitelju.
- Datoteke i pohrana: Poslužitelj datoteka za vašu tvrtku još je jedna uobičajena upotreba. To vam omogućuje da važne podatke držite na središnjem mjestu i postavite dopuštenja za kontrolu tko može pristupiti kojim datotekama.
- Usluge ispisa: Ako poduzeće ima desetke pisača u cijeloj zgradi, gubitak je vremena za IT osoblje da ih konfigurira pojedinačno za svaku novu radnu stanicu. Postavljanje poslužitelja za ispis omogućuje vam jednostavno mapiranje pisača na računala i smanjenje nepotrebnog rada.
- Usluge ažuriranja sustava Windows: često tvrtke ne žele da sva ažuriranja sustava Windows prođu odmah. Postavljanjem poslužitelja kao kontrolera Windows Update, možete usmjeriti sva ažuriranja radnih stanica putem tog poslužitelja i konfigurirati posebna pravila za njihov rad.

Ovo su samo neke od uloga poslužitelja koje Windows Server može podnijeti. Često će tvrtka imati više od jednog poslužitelja i podijeliti gore navedene uloge na više uređaja.

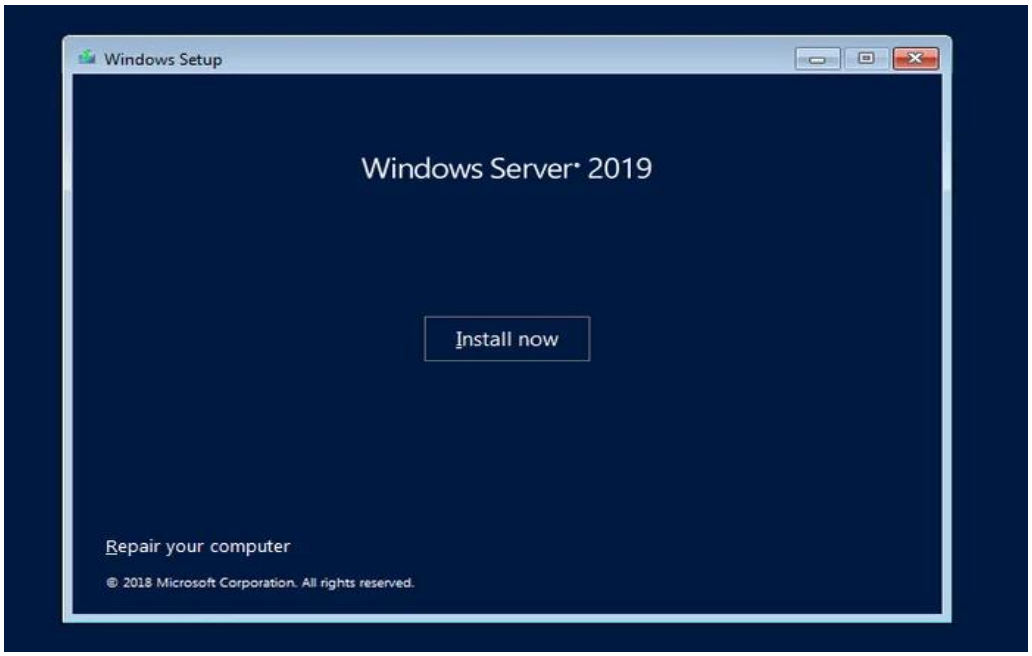
2.2 Instalacija Windows Server 2019

U par koraka opisat ćemo postupak instalacije Windows Servera 2019. Ne razlikuje se skoro ni po čemu od instalacije prošlih verzija.

Odaberemo jezik, vrijeme i format valute te layout tipkovnice. Stisnemo „Next“.

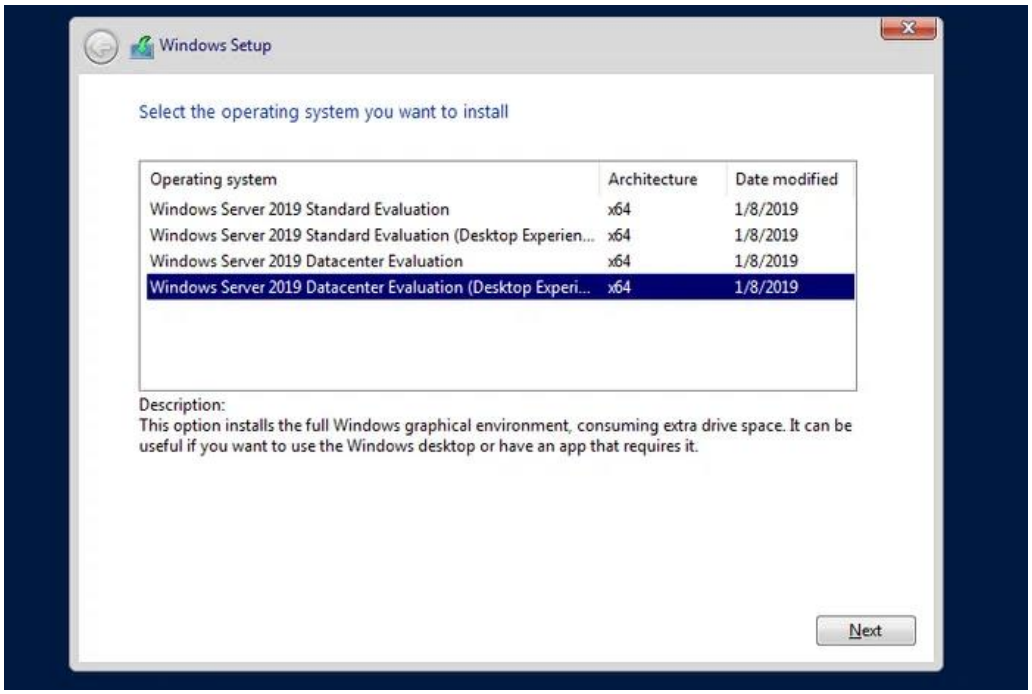


Slika 1 Windows Server 2019 setup



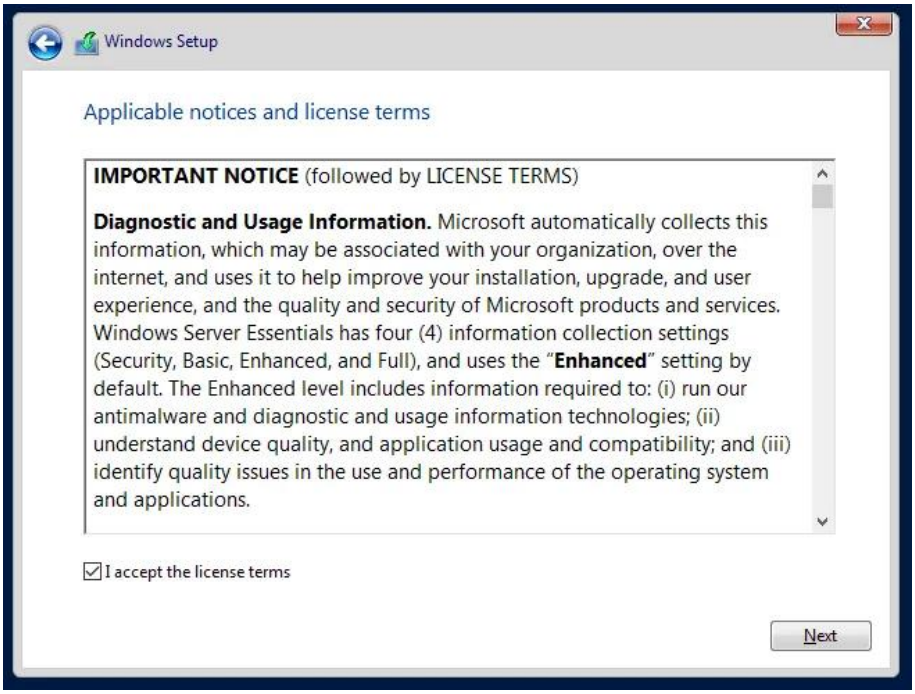
Slika 2 Windows Server 2019 setup

Odaberemo „Install now“.



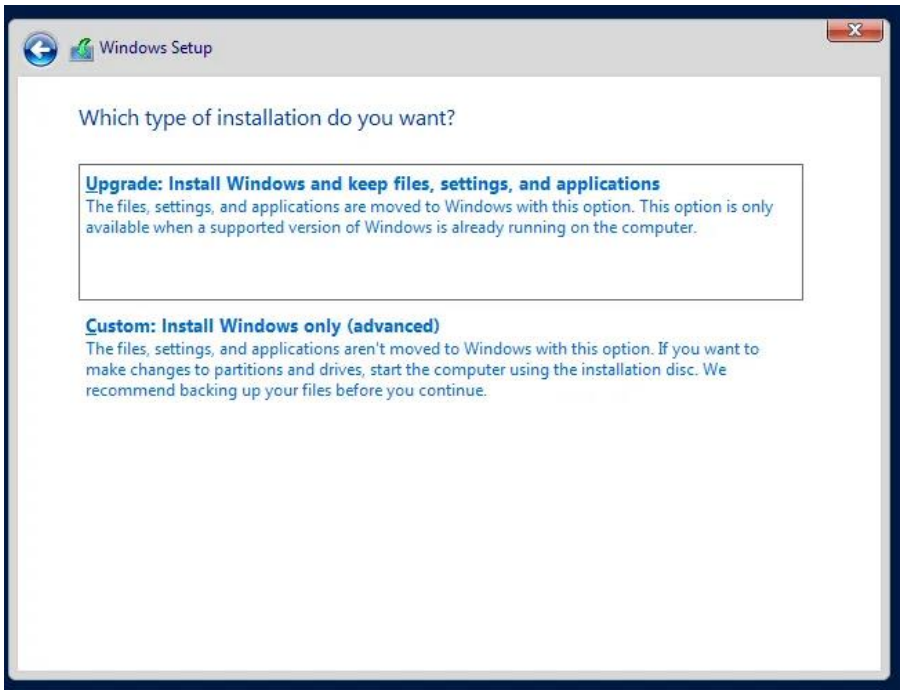
Slika 3 Odabir verzije Windows Servera

Odaberemo željenu verziju i stisnemo „Next“. U ovom završnom radu korištena je Standard Evaluation (Desktop Experience verzija).



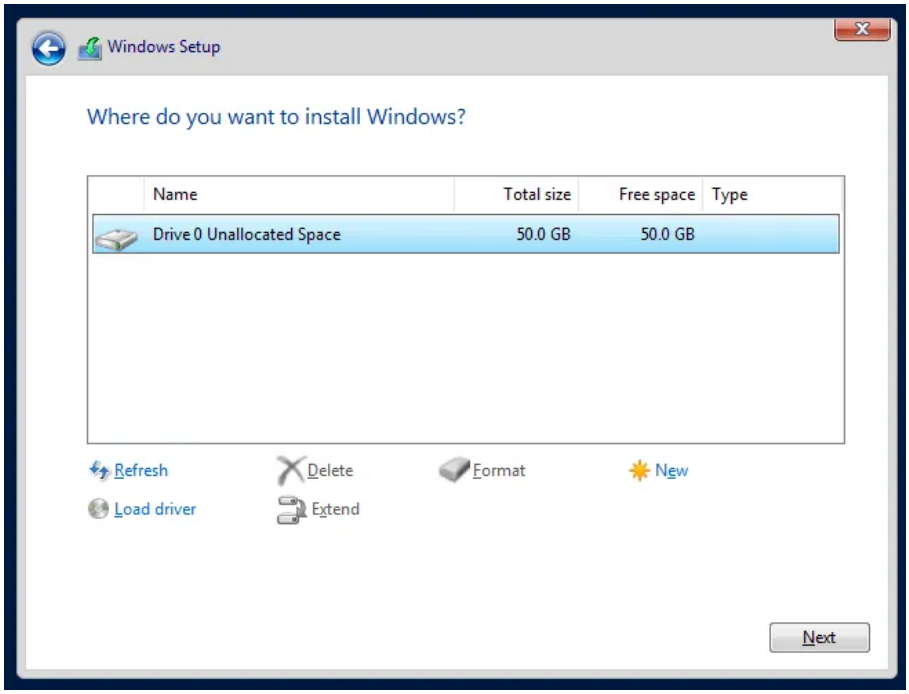
Slika 4 Windows setup

Odabrati „I accept the licence terms“, a prije toga pročitati uvjete i stisnuti „Next“.



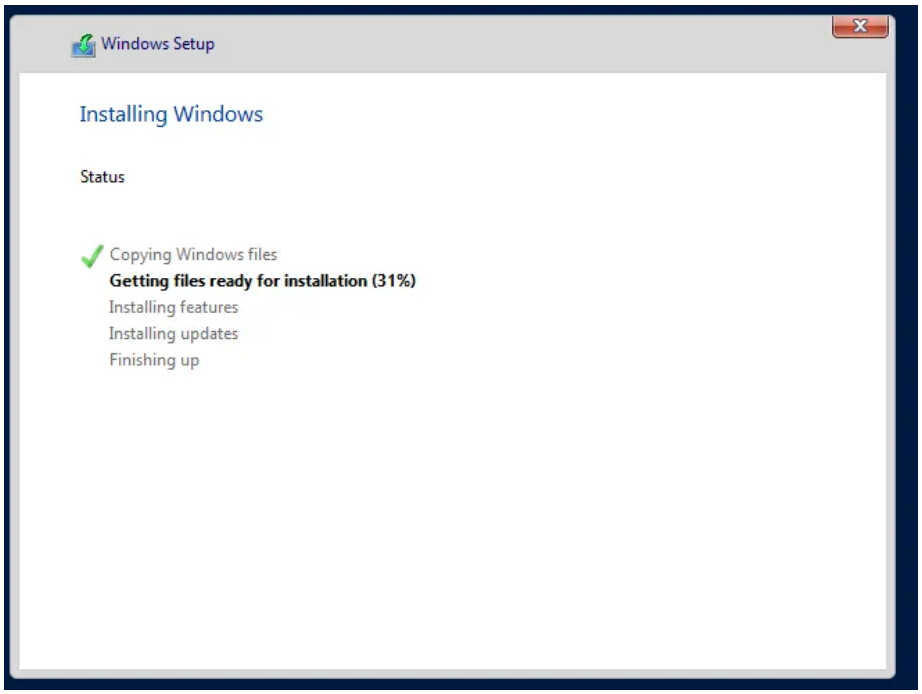
Slika 5 Windows Server opcije

Kod nove instalacije odabrati „Custom: Install Windows only (advanced)“. Ako se radi o upgrade-u (nadogradnji), odabrati prvu opciju.



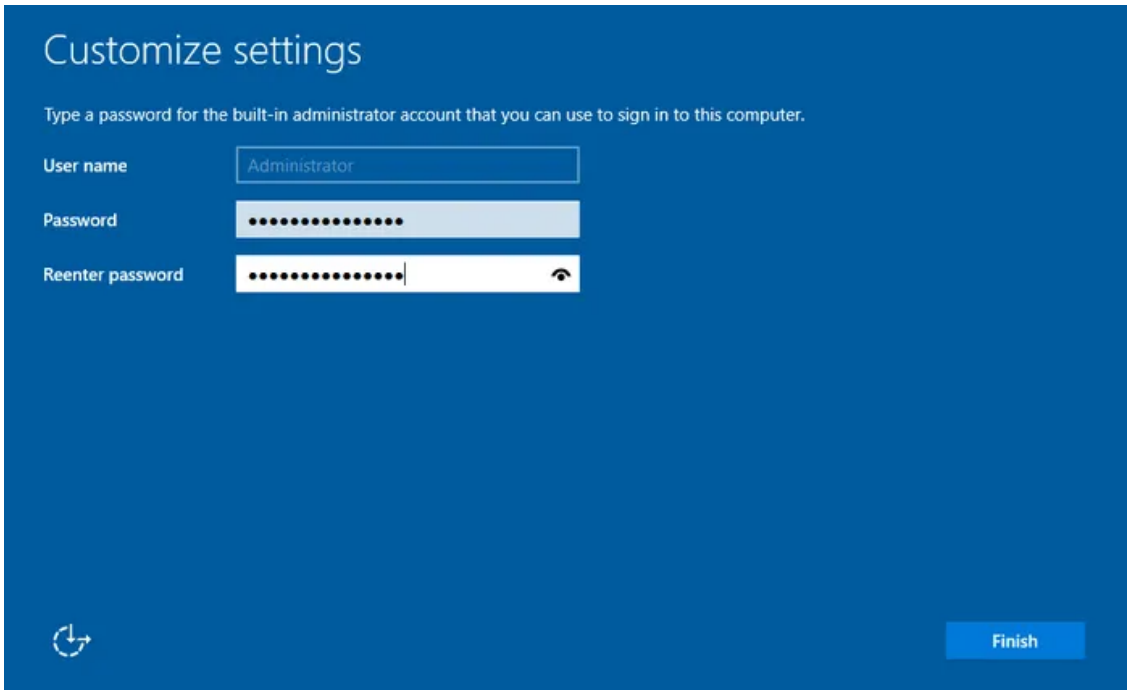
Slika 6 Windows Server podatkovno mjesto

Odabrati particiju na koju se želi instalirati, možemo opcionalno i ručno kreirati particije, no preporučljivo jest da kod nove instalacije Windows instalacija sama kreira particije. Stisnuti „Next“.



Slika 7 Windows Server instalacija

Instalacija je u tijeku. Sistem će se automatski ponovno pokrenuti kada je spreman i doći do ekrana za postavljanje administratorske lozinke.



Slika 8 Windows Server administratorska lozinka

Postavite administratorsku lozinku i pritisnite na „Finish“.

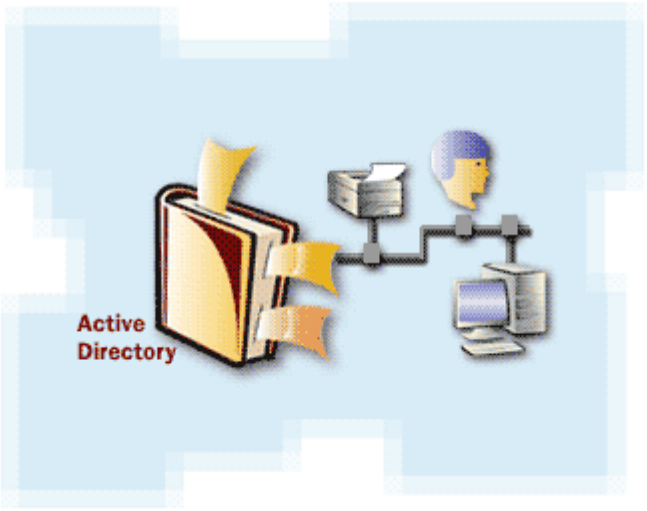
Slika 9 Windows Server 2019 zaključani ekran

Početni ekran za login korisnika. Pritisnike CTRL+ALT+DEL za login. Unesete lozinku i pokazat će se radna površina.

3. Active Directory

3.1 Općenito o Active Directory

Active Directory (AD) je baza podataka i skup usluga koje povezuju korisnike s mrežnim resursima koji su im potrebni za obavljanje posla.



Slika 10 Active Directory

Baza podataka (ili imenik) sadrži kritične podatke o vašem okruženju, uključujući korisnike i računala i tko što smije učiniti. Na primjer, u bazi podataka može se navesti 100 korisničkih računa s pojedinostima kao što su naziv posla, telefonski broj i lozinka svake osobe. Također će zabilježiti njihova dopuštenja.

Usluge kontroliraju velik dio aktivnosti koje se odvijaju u vašem IT okruženju. Konkretno, provjeravaju je li svaka osoba ono za što se pretpostavljaju (provjera autentičnosti), obično provjeravanjem korisničkog ID -a i lozinke koju unose te im dopuštaju pristup samo podacima koje smiju koristiti (autorizacija).

Active Directory pojednostavljuje život administratorima i krajnjim korisnicima, a poboljšava sigurnost organizacija. Korisnici se mogu autentificirati jednom, a zatim neometano pristupiti svim resursima u domeni za koju su ovlašteni (jednokratna prijava). Osim toga, datoteke se pohranjuju u središnje spremište gdje se mogu podijeliti s drugim korisnicima radi olakšavanja poslovanja.

Glavna usluga Active Directory je Active Directory Domain Services (AD DS), koja je dio operacijskog sustava Windows Server. Poslužitelji koji pokreću AD DS nazivaju se kontroleri domene (domain controller - DC). Organizacije obično imaju više domain controllera, a svaki ima kopiju imenika za cijelu domenu. Promjene u imeniku na jednom kontroleru domene - poput ažuriranja lozinke ili brisanja korisničkog računa - repliciraju se na druge domain controllere tako da svi ostaju ažurni. Poslužitelj globalnog kataloga je domain controller koji pohranjuje potpunu kopiju svih objekata u imenik svoje domene i djelomičnu kopiju svih objekata svih drugih domena u šumi (forest). To omogućuje korisnicima i aplikacijama pronalaženje objekata u bilo kojoj domeni njihove šume. Računala, prijenosna računala i drugi uređaji sa sustavom Windows (umjesto Windows poslužitelja) mogu biti dio okruženja Active Directory, ali ne pokreću AD DS. AD DS oslanja se na nekoliko uspostavljenih protokola i standarda, uključujući LDAP (Lightweight Directory Access Protocol), Kerberos i DNS (Domain Name System).

Važno je shvatiti da je Active Directory samo za lokalna Microsoftova okruženja. Microsoftova okruženja u oblaku koriste Azure Active Directory, koji služi istim. AD i Azure AD odvojeni su, ali mogu djelovati zajedno u određenoj mjeri ako vaša organizacija ima i lokalno i oblačno IT okruženje (hibridna implementacija).

3.2 Active Directory servisi

Servisi koji rade unutar Active Directory-a zapravo proširuju mogućnosti i iskoristivost samog Active Directory-a. Active Directory može upravljati strukturom direktorija, certifikatima i drugim servisima koji su namijenjeni za rad u serverskom okruženju, unutar mrežne strukture i domene.

3.2.1 Active Directory Lightweight Directory Services (AD LDS)

Ranije poznat kao Active Directory Application Mode (ADAM), implementacija je LDAP protokola za AD DS. AD LDS radi kao usluga na Windows poslužitelju. AD LDS dijeli bazu kodova s AD DS -om i pruža istu funkcionalnost, uključujući identičan API, ali ne zahtijeva stvaranje domena ili kontrolera domene. Omogućuje spremište podataka za pohranu podataka imenika i uslugu imenika sa sučeljem usluge LDAP imenika. Za razliku od AD DS -a, više AD LDS instanci može se izvoditi na istom poslužitelju.

LDAP aplikacijski je protokol koji se koristi za pristup i održavanje directory servisa unutar mreže. LDAP sprema objekte (korisnička imena i passworde), u directory servisima (Active Directory), i dijeli objekte kako je potrebno kroz mrežnu infrastrukturu kojom AD upravlja.

3.2.2 Certificate Services (AD CS)

Usluge certifikata Active Directory (AD CS) uspostavlja lokalnu infrastrukturu javnih ključeva. Može stvoriti, potvrditi i opozvati certifikate javnih ključeva za internu uporabu organizacije. Ti se certifikati mogu koristiti za šifriranje datoteka (kada se koriste s enkripcijskim datotečnim sustavom), elektroničke pošte (prema S/MIME standardu) i mrežnog prometa (kada ih koriste virtualne privatne mreže, sigurnosni protokol transportnog sloja ili protokol IPSec).

3.2.3 Active Directory Federation Service (AD FS)

Služi da bi se korisnik "predstavio" i da bi dobio pristup različitim dijelovima mreže, koristeći jednu prijavu (SSO, Single Sign-On). Možemo zaključiti da SSO koristimo radi lakše prijave korisnika, da se jednom prijavi u mreži, te da nakon uspješne prijave ima pristup dodijeljenim resursima unutar te mreže, odnosno Active Directory-a.

3.2.4 Rights Management (AD RMS)

Kontrolira sigurnost informacija, i upravljanje informacijama. Primjena ovog servisa može se pokazati na primjeru informacija u obliku elektroničke pošte (E-mail) ili Word dokumenata, odnosno drugih dokumenata koji se nalaze u mreži.

3.3 Struktura Active Directory

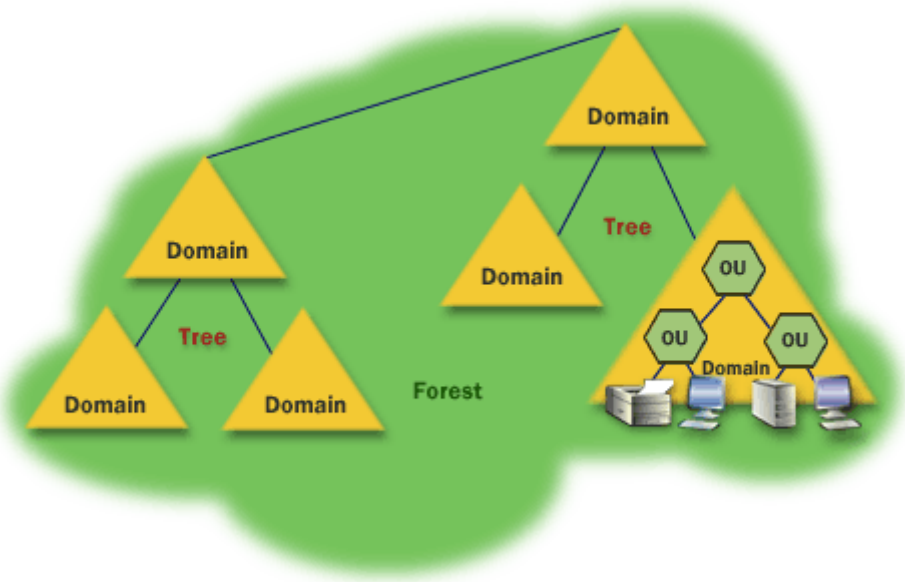
U Active Directory logička struktura odvojena je od fizičke strukture. Za organiziranje mrežnih resursa koristite logičku strukturu, a za konfiguraciju i upravljanje mrežnim prometom koristite fizičku strukturu. Fizička struktura Active Directory sastoji se od (web) mjesta i kontrolera domene.

3.3.1 Logička struktura

Glavna područja logičke strukture Active Directory-a uključuju:

- Domene (Domain)
- Organizacijske jedinice (UO)
- Stabla (Trees)
- Šume (Forests)

Na slici možete vidjeti njihov međusobni odnos.

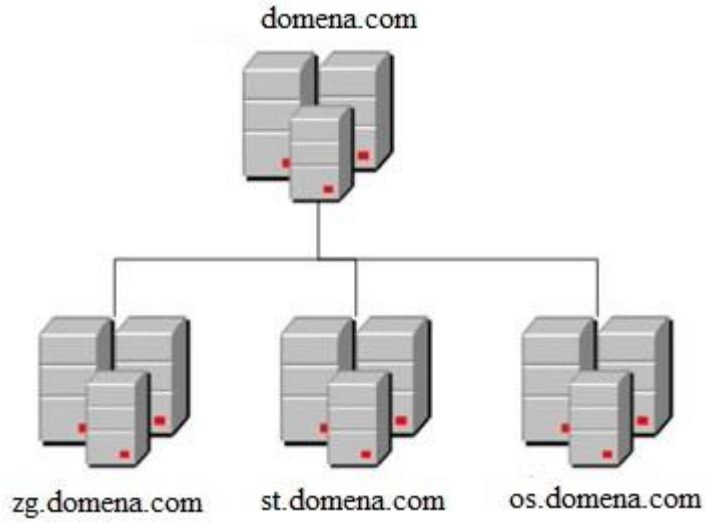


Slika 11 Domena, organizacijske jedinice, drveće, šuma

Active Directory se zasniva na sloju domena, stabala (Trees) i šuma (Forests) za upravljanje mrežnim elementima. Domena je grupa objekata (korisnici i uređaji), koji dijele istu Active Directory bazu. Domene imaju domain name system (DNS) strukturu.

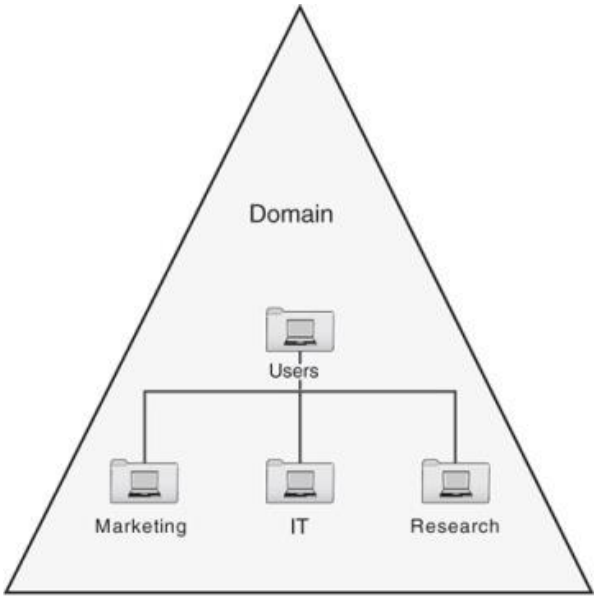
Domena je osnovna jedinica za grupiranje povezanih objekata u Active Directory-u. Obično domene odgovaraju odjelima u tvrtki. Na primjer, tvrtka s odvojenim odjelima za

računovodstvo, proizvodnju i prodaju mogla bi imati domene računovodstvo, proizvodnja i prodaja. Domene mogu odgovarati i zemljopisnim lokacijama. Na primjer, tvrtka s uredima u Zagrebu, Split i Osijeku mogla bi imati domene pod nazivom zg, st i os.



Slika 12 Domene

Mnoge domene imaju previše objekata za upravljanje zajedno u jednoj grupi. Srećom, Active Directory omogućuje stvaranje jedne ili više *organizacijskih jedinica*, poznatih i kao UO. Organizacijske jedinice omogućuju organiziranje objekata unutar domene, bez dodatnog rada i neučinkovitosti stvaranja dodatnih domena.



Slika 13 Organizacijske jedinice

Jedan od razloga za stvaranje organizacijskih jedinica unutar domene je taj što možete dodijeliti administrativna prava svakoj organizacijskoj jedinice zasebno i po želji. Zatim ti

korisnici mogu obavljati rutinske administrativne zadatke, poput stvaranja novih korisničkih računa ili poništavanja lozinki.

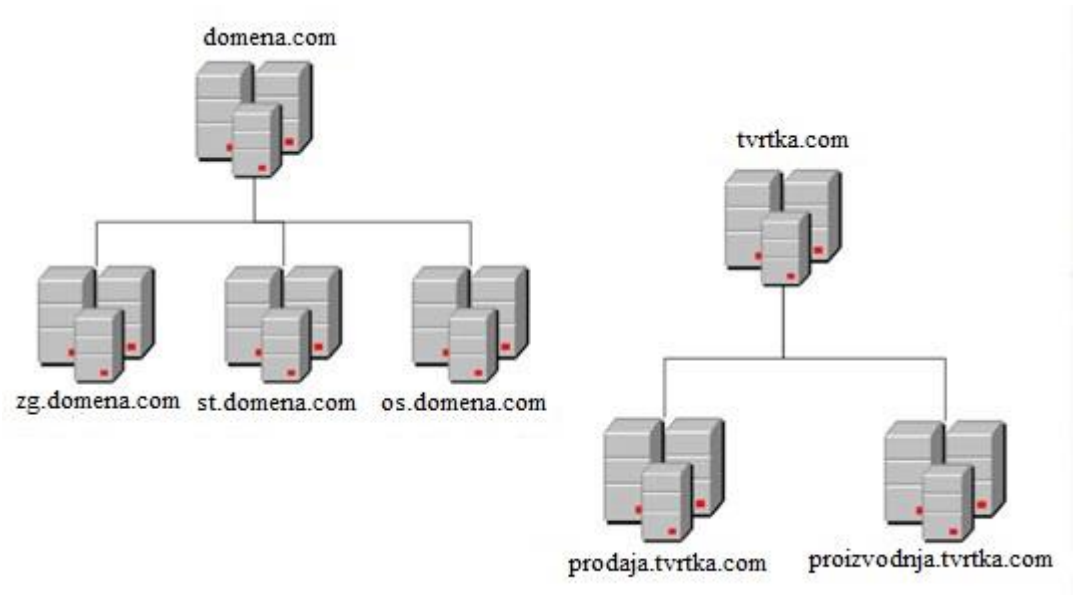
Na primjer, pretpostavimo da se u domeni ureda u Splitu, nazvanoj st, nalaze računovodstveni i pravni odjeli. Umjesto stvaranja zasebnih domena za te odjele, mogli biste stvoriti organizacijske jedinice za odjele.

Stablo je skup imena Active Directory-a koji dijele zajednički prostor imena. Na primjer, domene domena.com, zg.domena.com, st.domena.com i os.domena.com čine stablo (tree) izvedeno iz zajedničke korijenske domene, domena.com.

Šuma (forest) je skup stabala. Drugim riječima, šuma je zbirka jednog ili više stabala domene koja ne dijele zajedničku nadređenu domenu.

Na primjer, pretpostavimo da domena.com kupuje neku drugu tvrtku, koja već ima vlastitu korijensku domenu pod nazivom tvtka.com, s nekoliko vlastitih poddomena. Zatim možete stvoriti šumu od ova dva stabla domene kako bi domene mogle vjerovati jedna drugoj.

Ključ šuma Active Directory-a je baza podataka koja se naziva globalni katalog. Globalni katalog je vrsta super-direktorija koji sadrži podatke o svim objektima u šumi, bez obzira na domenu. Zatim, ako se korisnički račun ne može pronaći u trenutnoj domeni, u globalnom se katalogu traži taj račun. Globalni katalog nudi referencu na domenu u kojoj je račun definiran.



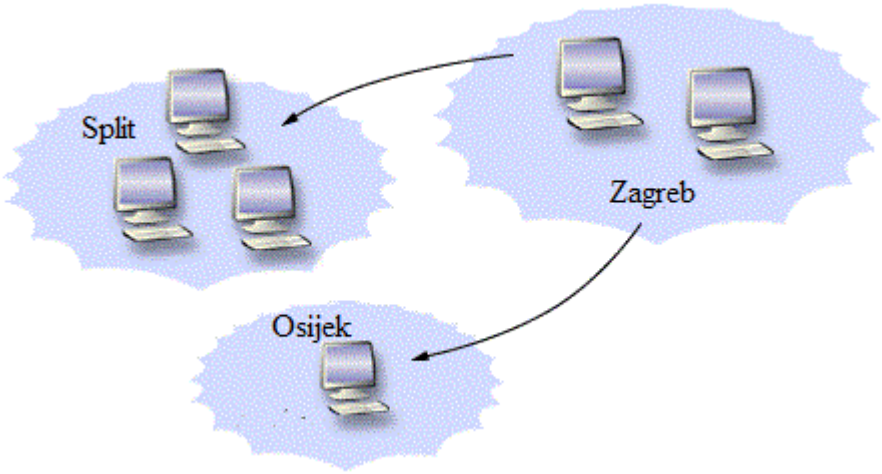
Slika 14 Šuma

3.3.2 Fizička struktura

Mjesta su fizičke (a ne logičke) grupe definirane jednom ili više IP podmreža. Definicije mjesta neovisne su o domeni i strukturi organizacijskih jedinica i uobičajene su u cijeloj šumi. Mjesta se koriste za kontrolu mrežnog prometa generiranog replikacijom, a također i za upućivanje klijenata na najbliže kontrolere domene (DC).

Dizajniranje topologije web mjesta za domenske usluge Active Directory (AD DS) uključuje planiranje postavljanja kontrolera domene i projektiranje web mjesta, podmreža, veza na web stranice i mostova veza na web lokaciju kako bi se osiguralo učinkovito usmjeravanje prometa upita i replikacije.

Prije nego počnete dizajnirati topologiju web mjesta, morate razumjeti fizičku mrežnu strukturu. Osim toga, najprije morate dizajnirati logičku strukturu Active Directory-a, uključujući administrativnu hijerarhiju, plan šuma i plan domene za svaku šumu.



Slika 15 Fizička struktura

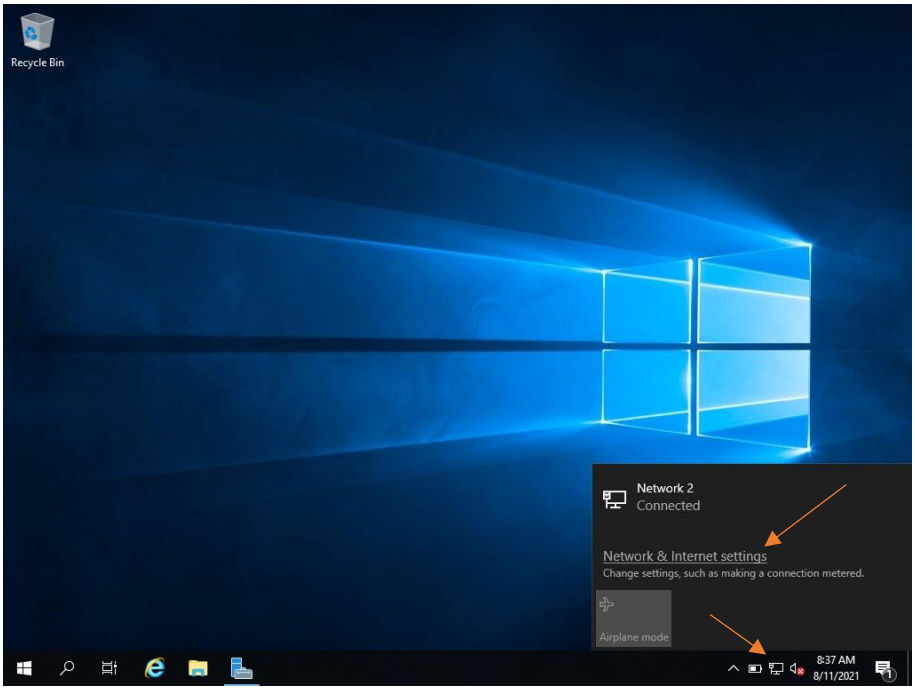
3.4 Instalacija Active Directory

Sada kada smo upoznati s Windows Serverom, Active Directory-em, njegovim funkcijama i strukturama, došli smo do instalacije, odnosno prvotnog postavljanja Active Directory-a na Windows Server 2019.

Prije nego što počnemo konfigurirati Active Directory na poslužitelju, moramo provjeriti dali je mrežnom adapteru poslužitelja dodijeljena valjana statička IP adresa na lokalnoj mreži.

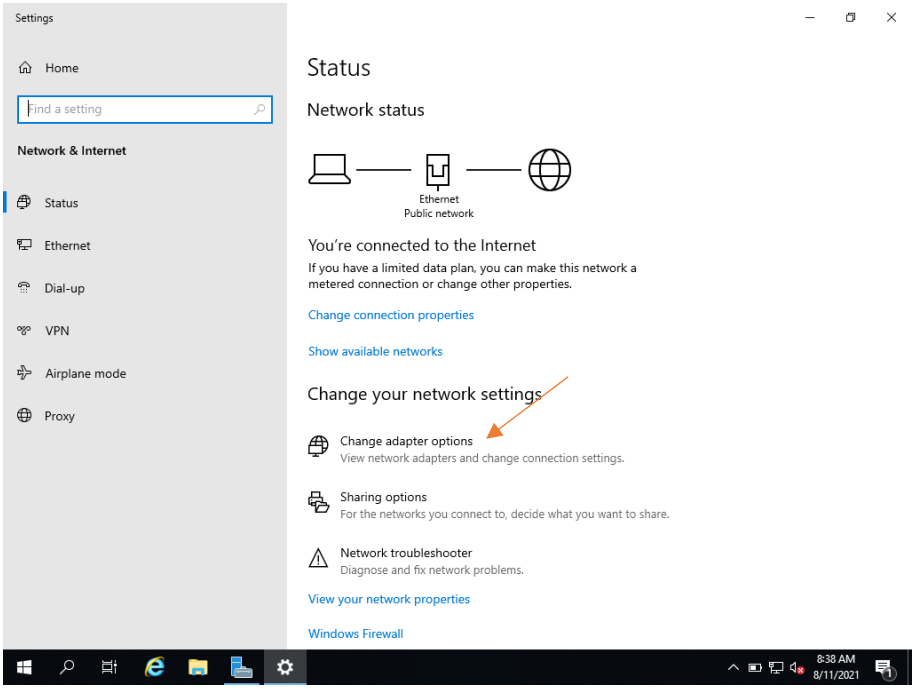
3.4.1 Konfiguracija statičke IP adrese

Potrebno je logirati se u Windows Server kao administrator. Zatim se klikne mišem u donjem desnom kutu u system trayu na ikonu mrežne veze, te odabrati „Network & Internet Settings“.



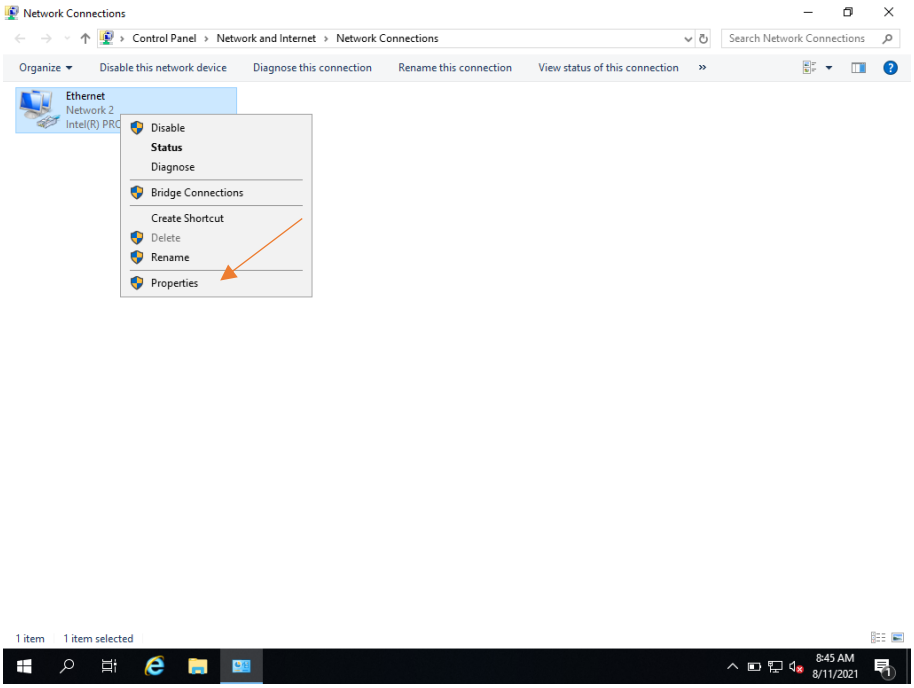
Slika 16 Network & Internet opcije

U sljedećem prozoru koji se otvori odaberem „Change adapter options“.



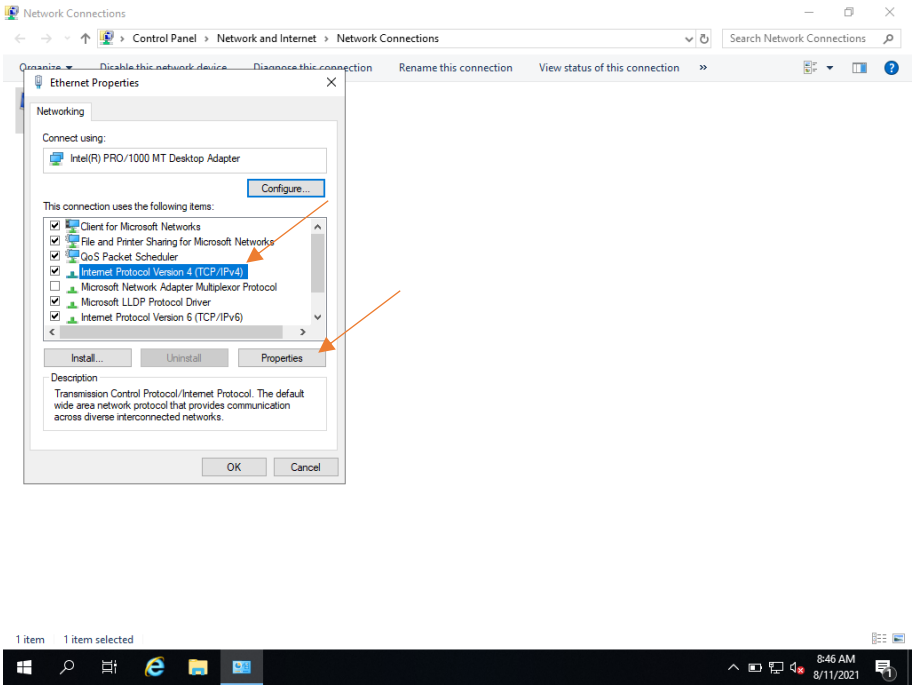
Slika 17 Change adapter options

Otvorit će se sljedeći prozor. Pronađemo „Ethernet“ mrežni adapter te desnim klikom miša stisnemo na njega i odaberemo „Properties“.



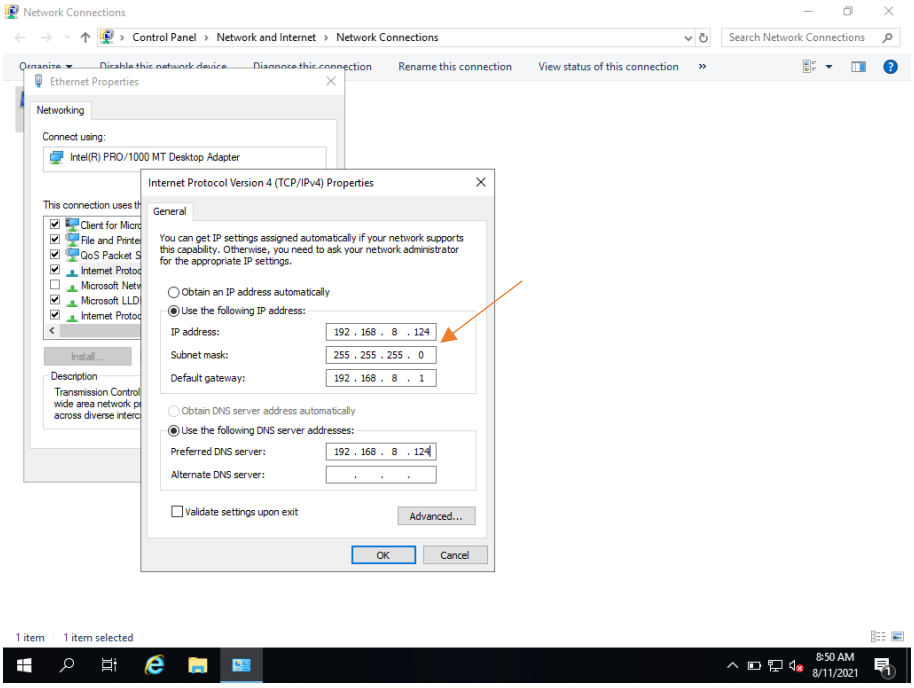
Slika 18 Ethernet

Odaberemo „Internet Protocol Version 4 (TCP/IPv4)“, te stisnemo „Properties“.



Slika 19 Internet Protocol Version 4

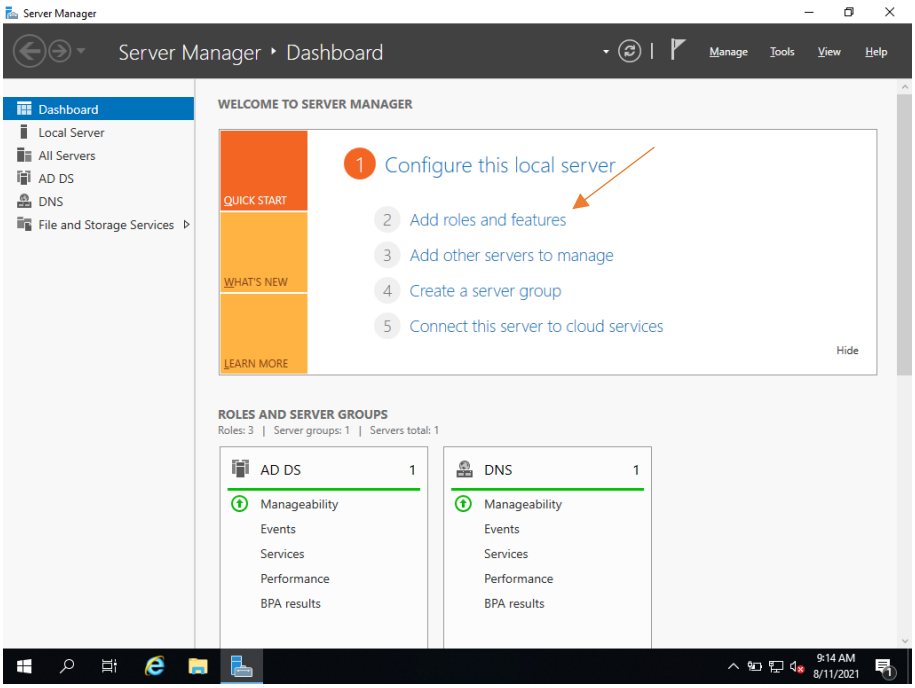
Otvorit će se prozor u kojem ručno unosimo željenu mrežnu adresu, subnet masku te adresu usmjernika (routera). Pod DNS postavke unosimo, najbolje, IP adresu poslužitelja, pošto će on u ovom slučaju biti i DNS server.



Slika 20 IPv4 postavke

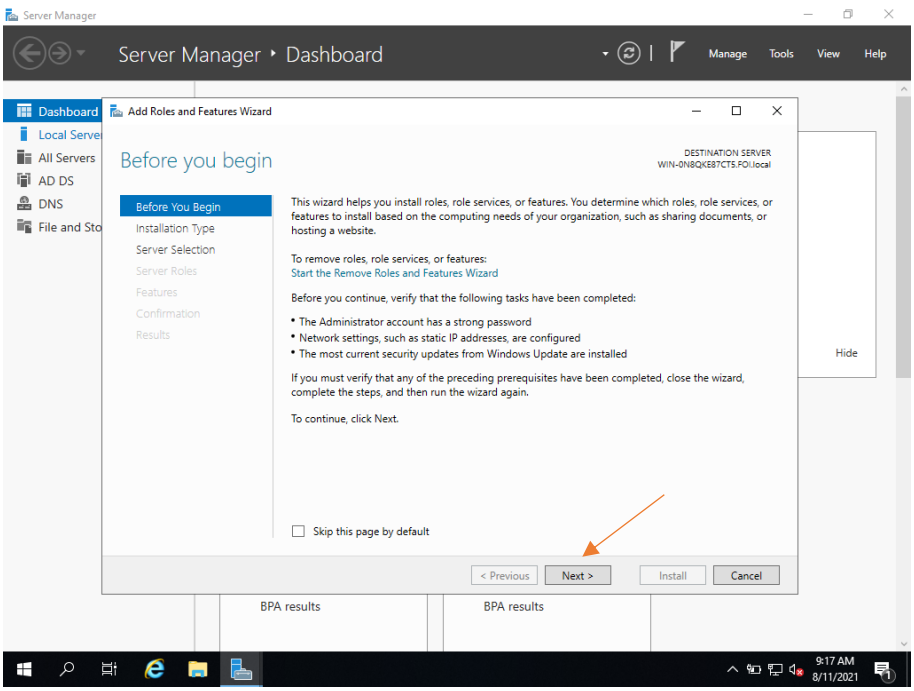
3.4.2 Server Manager

Nakon što smo postavili statičku IP adresu poslužitelju, odlazimo u Server Manager.



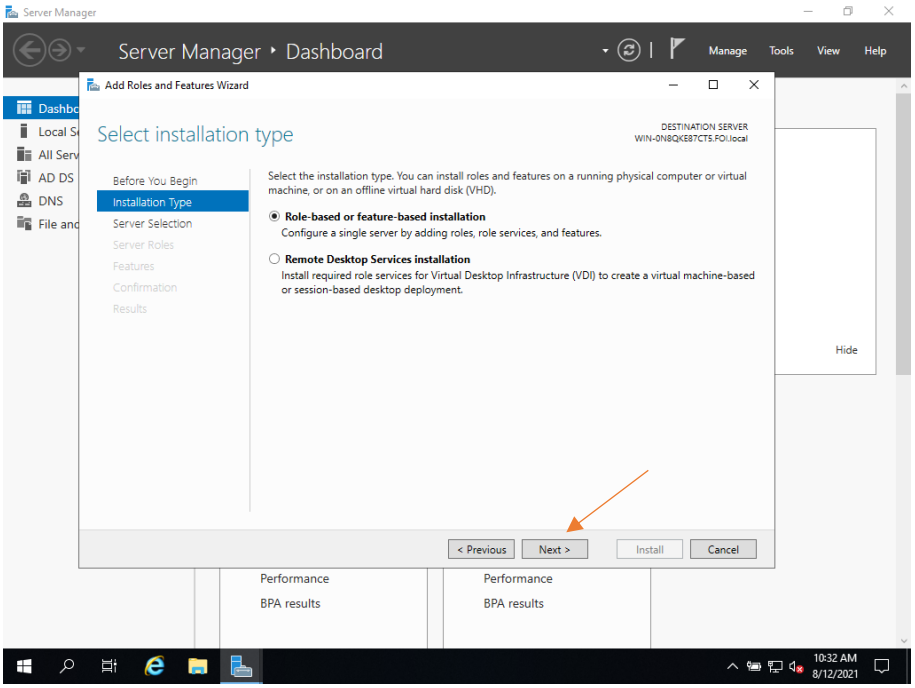
Slika 21 Server Manager

Kako bi započeli konfiguraciju Active Directory, unutar Server Managera odaberemo „Add roles and features“ i stisnemo „Next“.



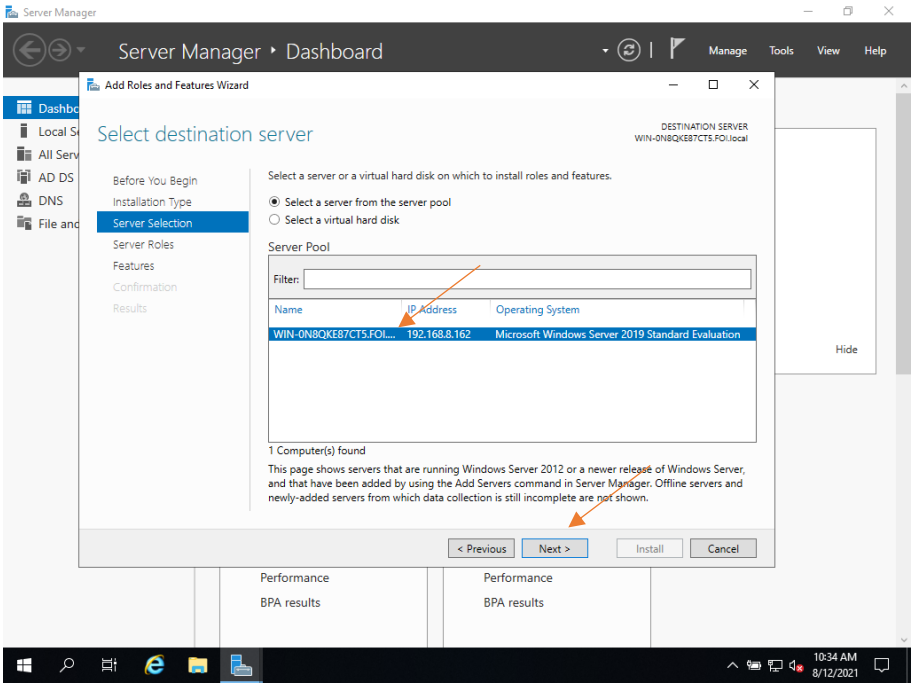
Slika 22 Active Directory instalacija

Nakon pritiska na gumb „Next“ pojavljuje se prozor za odabir načina instalacije. Odaberemo „Role-based or feature-base installation“ nakon čega se klikne na gumb „Next“.



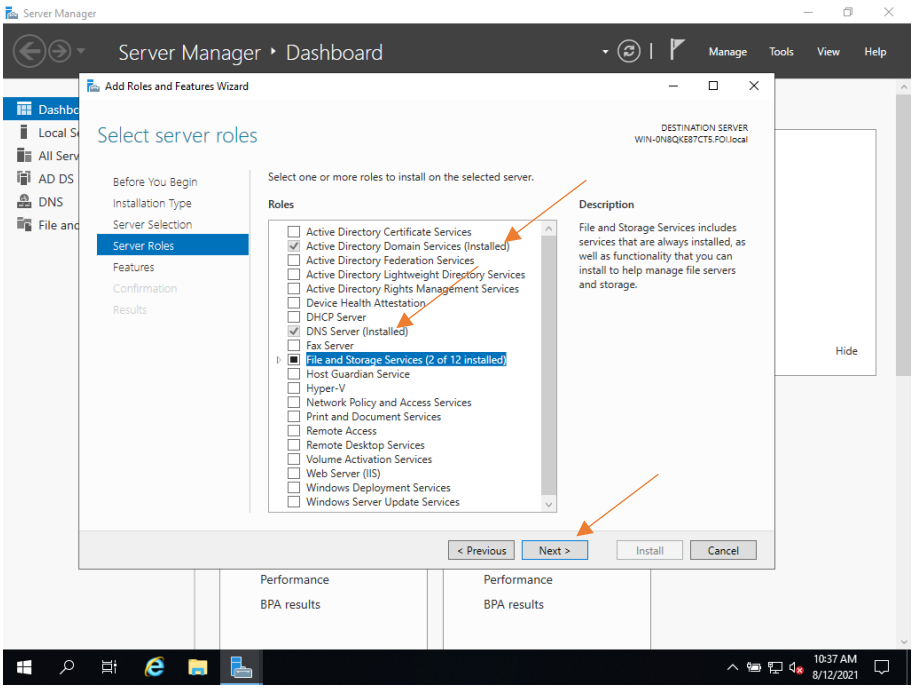
Slika 23 Role-based or feature-base installation

U ovoj fazi pod nazivom "Select destination server", odaberemo poslužitelj na koji želimo instalirati Active Directory i kliknemo „Next“.



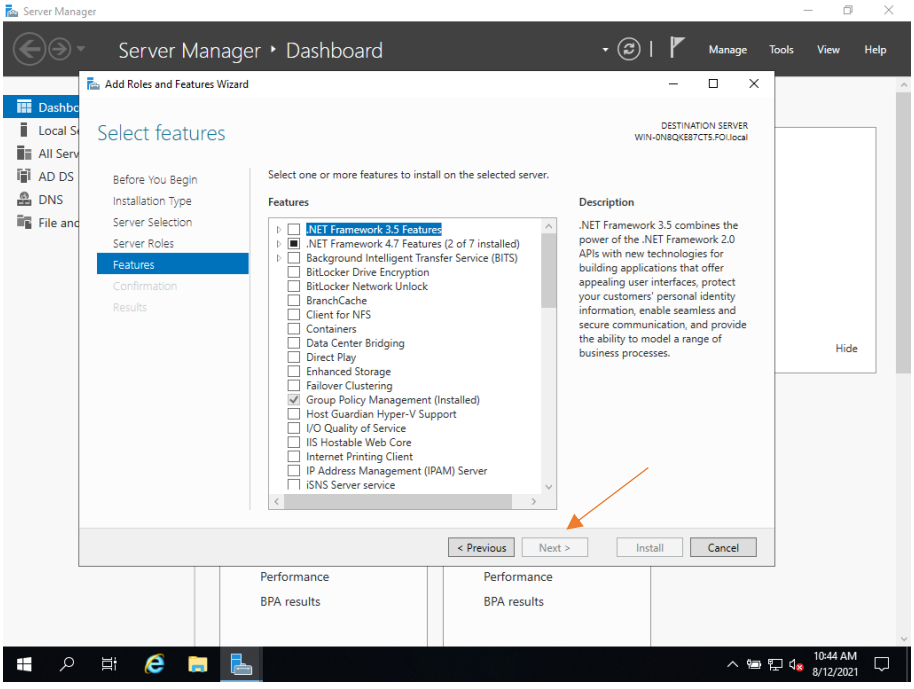
Slika 24 Odaberite željeni server

Ovdje ćete vidjeti mnoge opcije za odabrati/instalirati. Kao što možete pogoditi, odabrat ćemo „Active Directory Domain Services“. Opcionalno, ako ćete koristiti, možete odabrati i DNS Server. Kliknemo „Next“.



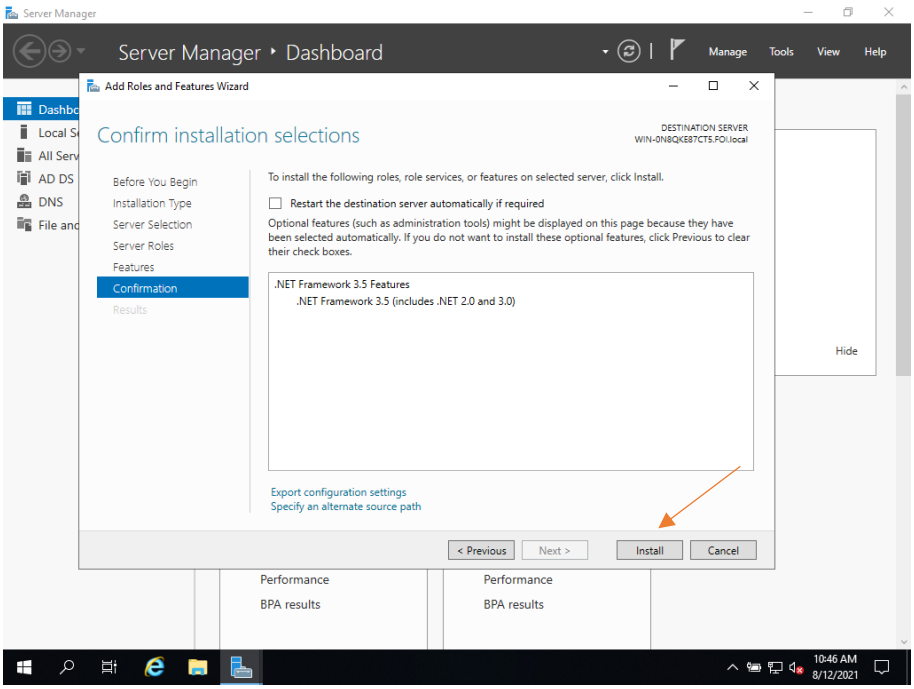
Slika 25 Usluge domene Active Directory 1

Na ovoj stranici samo pritisnite „Next“.



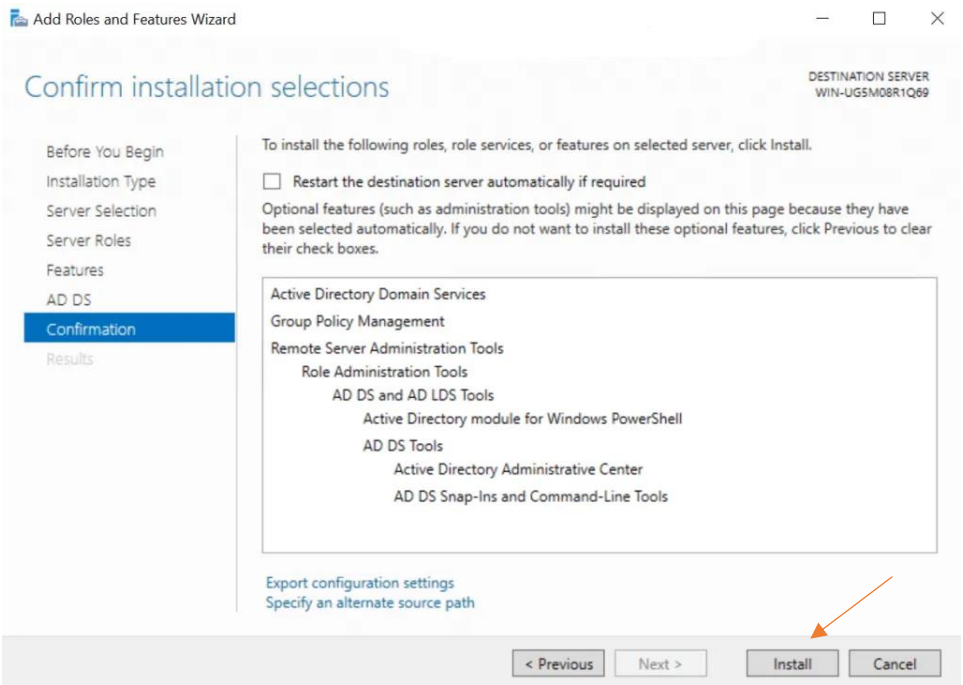
Slika 26 Usluge domene Active Directory 2

Na ovoj stranici stisnemo „Install“.



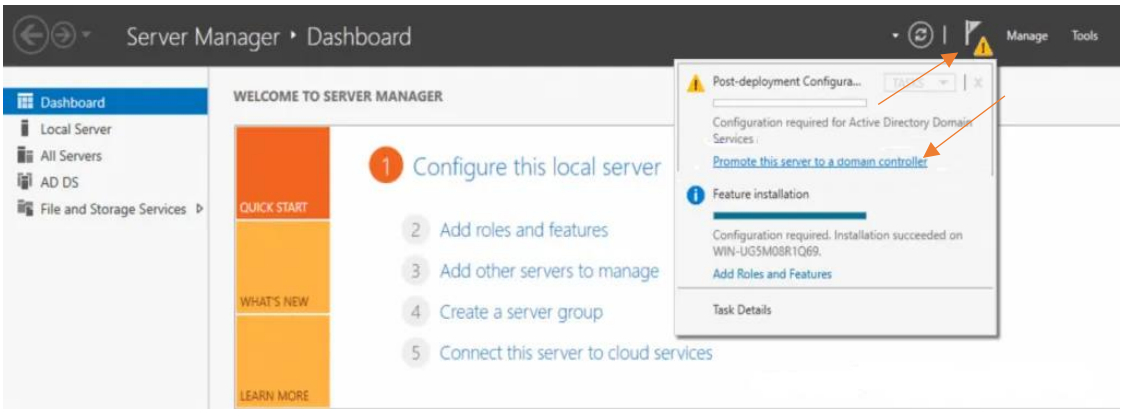
Slika 27 Active Directory instalacija 1

Pregled svih odabira prije instalacije Active Directory. Stisnuti „Install“.



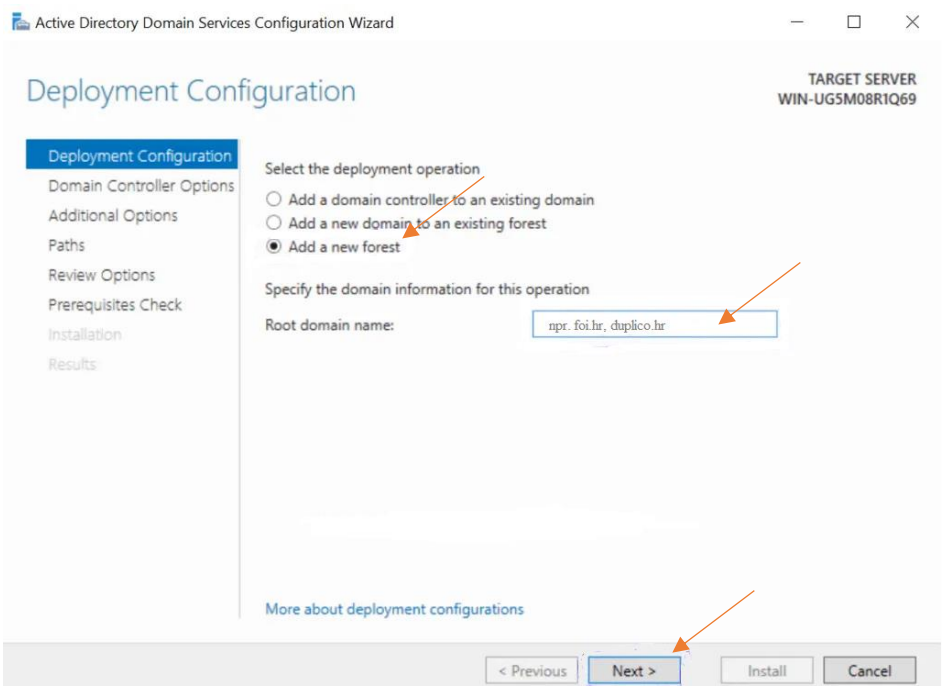
Slika 28 Active Directory instalacija 2

Nakon što smo uspješno prikazali i završili s instaliranjem domenskih usluga Active Directory, posljednji je korak promovirati poslužitelj u „Domain controller“ (DC). U gornjem desnom kutu „Server Managera“ ćete primijetiti žuti usklik uz karticu "Manage" kao što je prikazano na slici 29. Kliknite na nju i odaberite "Promote this server to a domain controller".



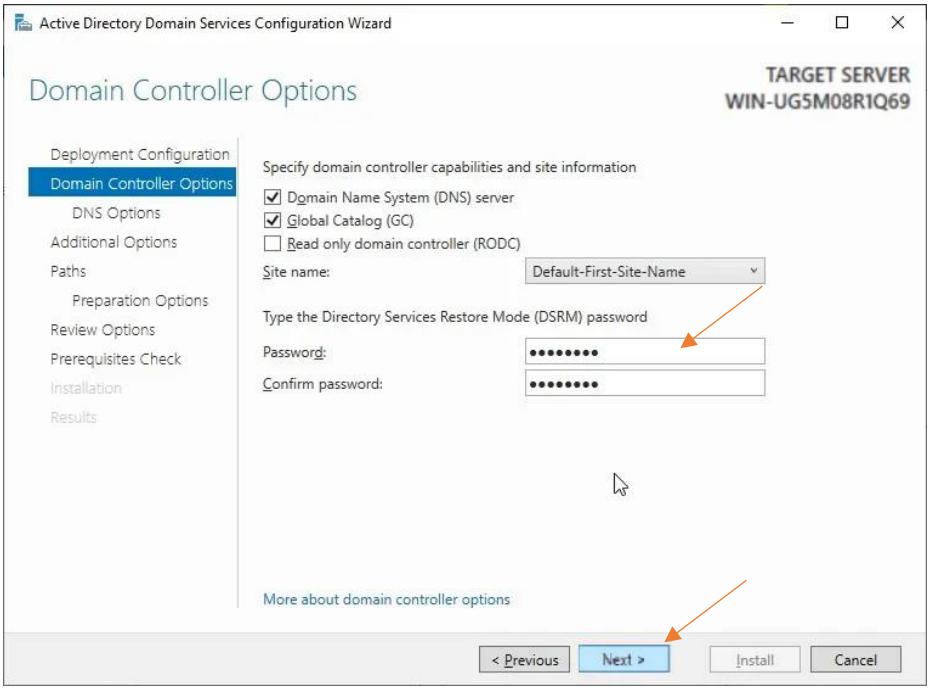
Slika 29 Domain controller

Pojavit će se novi prozor pod nazivom “Active Directory Domain Services Configuration Wizard”, kao što je prikazano u nastavku. Dodati ćemo novu šumu, ali u slučaju da želite učiniti nešto drugačije u ovom koraku, slobodni ste odabrati druge opcije. Dodajte naziv korijenske domene svoje organizacije, npr. foi.hr. Kliknite "Next" nakon što odaberete svoj izbor.



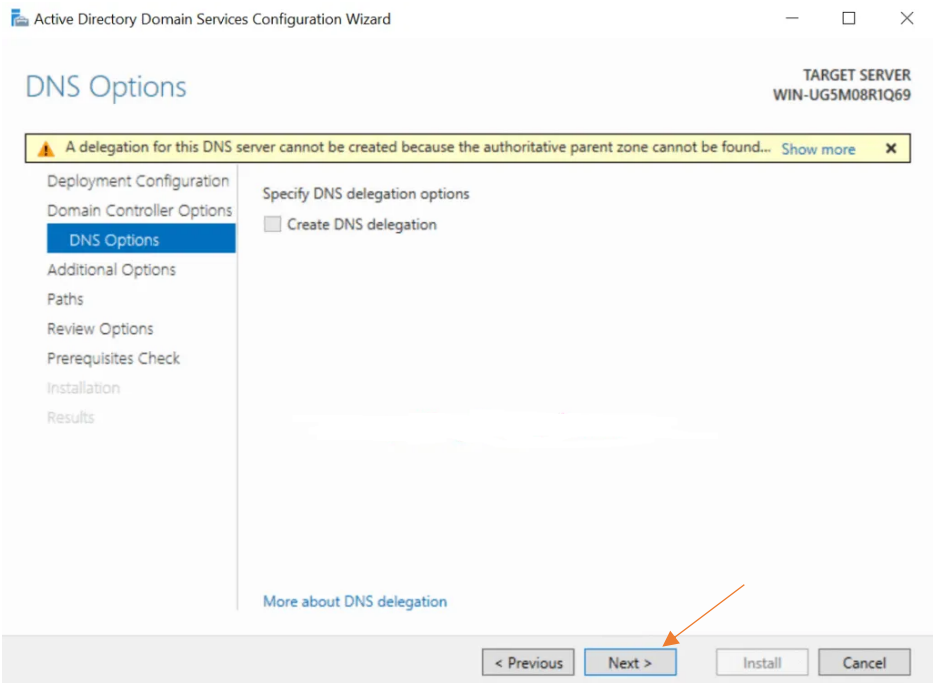
Slika 30 Active Directory Domain Services Configuration Wizard

Na opcijama Domain Controller ostavite označene zadane vrijednosti i unesite svoju lozinku. Nakon toga kliknite "Next"



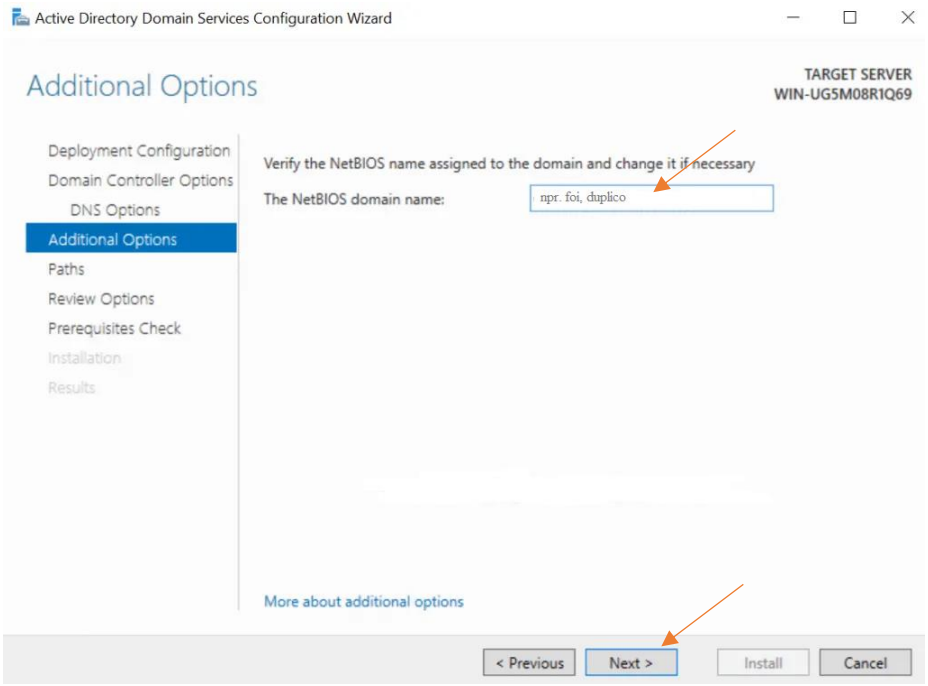
Slika 31 Domain Controller opcije

Na sljedećoj stranici „DNS Options“ vjerojatno ćete na vrhu vidjeti pogrešku „A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found". Zanemarite i kliknite "Next“.



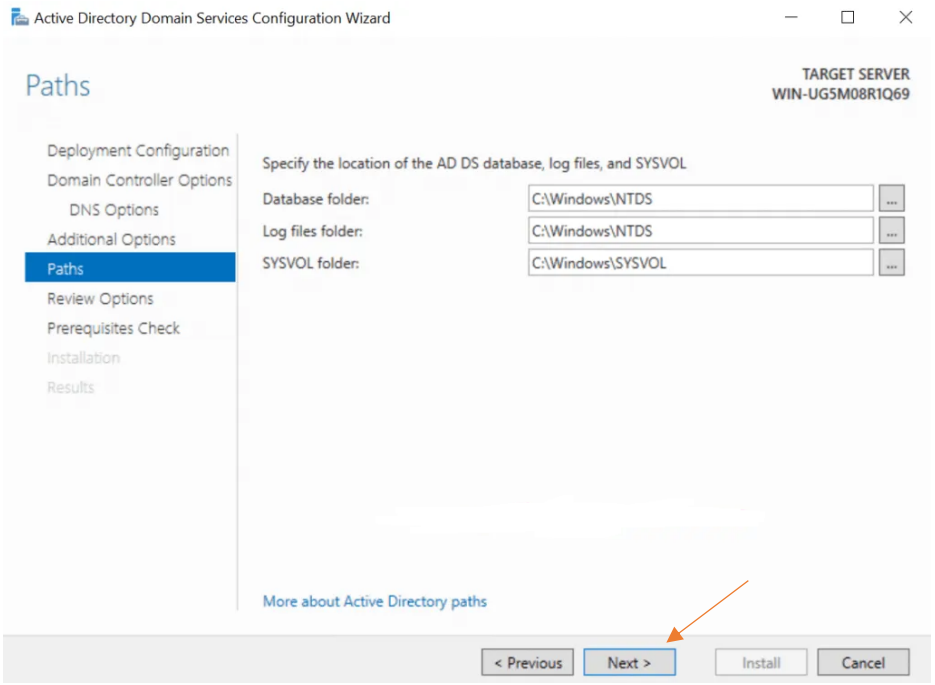
Slika 32 DNS opcije

Na sljedećoj stranici, slika 33, ostavite naziv domene NetBIOS kao zadani ili ga možete promijeniti sve dok ne bude dulji od 15 znakova. Nakon toga kliknite "Next".



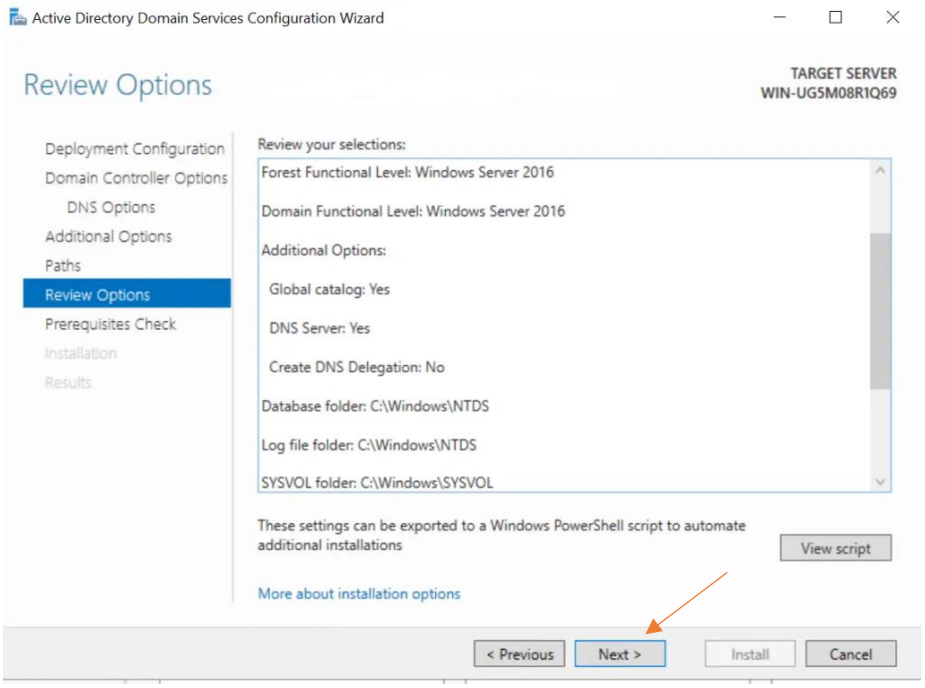
Slika 33 NetBios

Ostavite putanje kako su zadane i kliknite "Next" kao što je prikazano u nastavku.



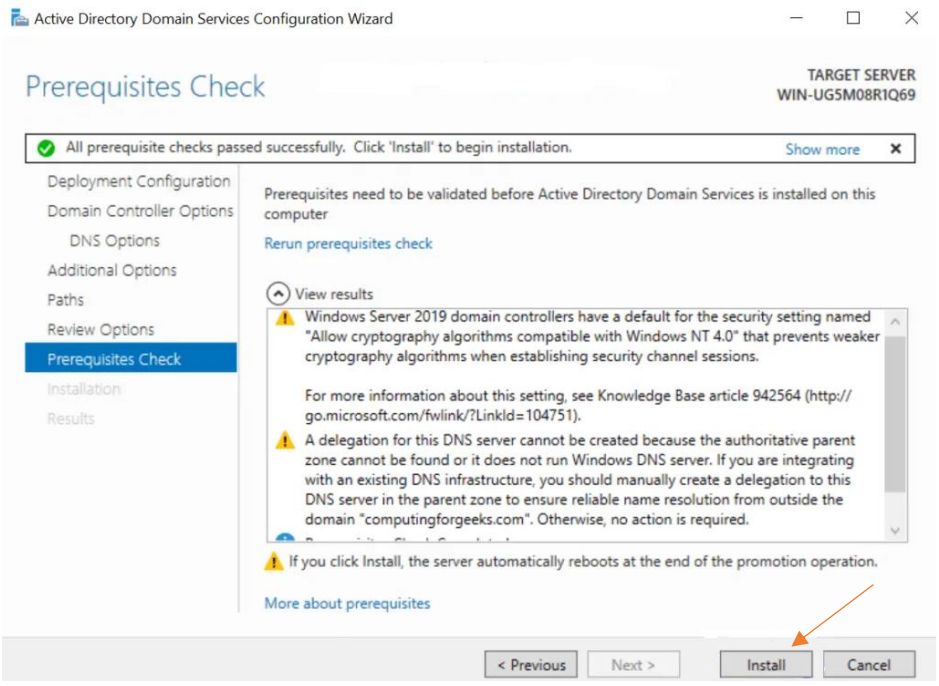
Slika 34 Domain Controller instalacija 1

U ovom koraku poslužitelj vam omogućuje da pregledate ono što ste do sada učinili. Pregledajte još jednom odabire i ako se slažete s istima pritisnite "Next".



Slika 35 Domain Controller instalacija 2

U ovom koraku preduvjeti će se provjeriti prije nego što se instaliraju domenske usluge Active Directory. Ako ovdje dobijete bilo kakvu pogrešku, pogledajte je i ispravite bilo što u prethodnim koracima. Ako je sve u redu, kliknite "Install".



Slika 36 Domain Controller instalacija 3

Nakon toga će se poslužitelj ponovno pokrenuti i spremni ste logirati se kao „Administrator“, kreirati korisnike, dodavati računala u domenu te početi sa implementacijom GPO (Group policy object), odnosno sigurnosnih politika.

4. Implementacija sigurnosnih politika

U ovom poglavlju nećemo se doticati „Sigurnosnih politika“ kao dokumenta, no, bez sigurnosnih politika, odnosno skupa pravila i smjernica što, kako i gdje želimo ograničiti, zaštititi, ne možemo ni jasno znati kako da postavimo naš informacijski sustav. Stoga ćemo vrlo ukratko dotaknuti se „Sigurnosnih politika“. Prikazat ćemo kako se kreiraju organizacijske jedinice unutar Active Directory-a, korisnici, kako se dodaje računalo u domenu te na koji način kreiramo, odnosno definiramo sigurnosna pravila, tj. primjenu istih.

Informacijski sustav ne može se u potpunosti zaštiti i to je činjenica koje mora biti svjestan svaki korisnik. Radnje odgovornih osoba u cilju povećanja sigurnosti sustava vrlo su individualne zbog individualnosti samih informacijskih sustava i stoga se ne mogu definirati univerzalne radnje prema kojima bi se gradila sigurnost sustava. Individualnost je u planiranju sigurnosti i vrlo preporučljiva, jer se na taj način otežava planiranje i izvršavanje napada od strane zlonamjernih korisnika.

Sigurnosna politika je skup pravila, smjernica i postupaka koja definiraju na koji način informacijski sustav učiniti sigurnim i kako zaštititi njegove vrijednosti, tehnološke i informacijske. Ona govori korisnicima što smiju raditi, što ne smiju raditi, što moraju raditi i koja je njihova odgovornost. Svakodnevnim razvojem tehnologija otkrivaju se i nove metode kojima je moguće ugroziti sustav. Stoga definiranje općenite sigurnosne politike za informacijske sustave nije moguće i jednom napisana politika mora se redovito pregledavati, mijenjati i nadopunjavati kada se za tim ukaže potreba.

4.1 Group policy object (GPO)

Group policy značajka su sustava Windows koja omogućuje širok izbor naprednih postavki koje mrežni administratori mogu koristiti za kontrolu radnog okruženja korisnika i računa unutar Active Directory-a. U osnovi pruža centralizirano mjesto administratorima za upravljanje i konfiguriranje operacijskih sustava, aplikacija i korisničkih postavki.

Group Policy Object (GPO) skupina je postavki koje se stvaraju pomoću Group Policy Editora. Group Policy Object-i mogu biti povezani s jednim ili brojnim spremnicima Active Directory-a, uključujući web lokacije, domene ili organizacijske jedinice (OU).

Na primjer, GPO može pomoći u provedbi politike najmanjih privilegija gdje vaši korisnici imaju samo dopuštenja potrebna za obavljanje svog posla. To mogu učiniti onemogućavanjem globalnih administratorskih prava u vašoj mreži i dodjeljivanjem administratorskih privilegija pojedincima ili grupama na temelju njihovih uloga.

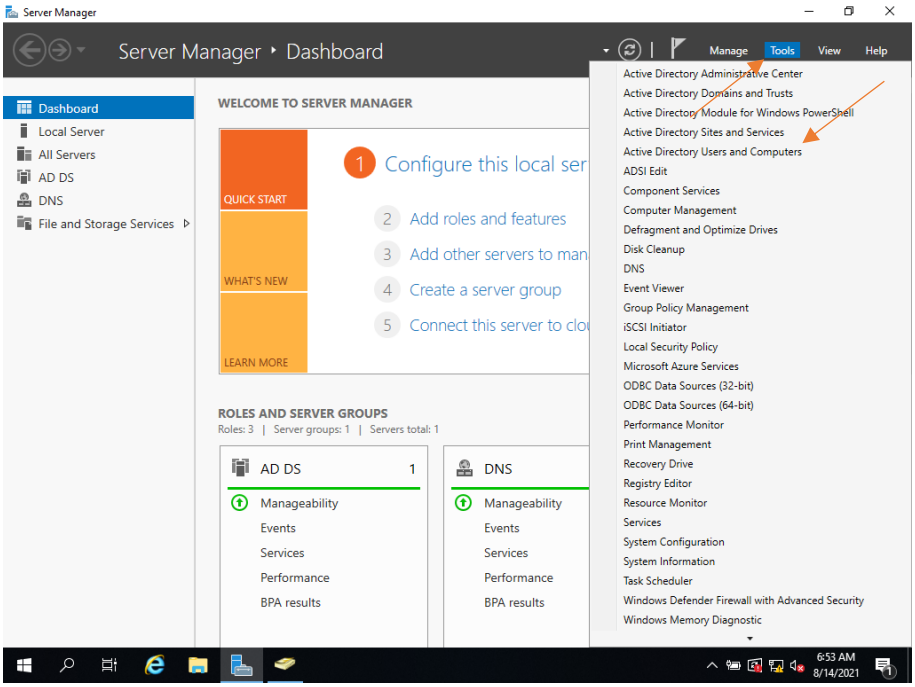
Grupna se pravila mogu koristiti na brojne načine za jačanje sigurnosti, uključujući onemogućavanje zastarjelih protokola, sprječavanje korisnika da unose određene promjene i još mnogo toga.

Mnoge organizacije rade s opuštenim pravilima zaporki, a mnogi korisnici često postavljaju zaporke koje nikada ne istječu. Zaporke koje se ne rotiraju redovito, previše su jednostavne ili koriste uobičajene lozinke u opasnosti su od hakiranja grubom silom. GPO-ovi se mogu koristiti za utvrđivanje duljine lozinke, složenosti i drugih zahtjeva.

GPO-i se mogu koristiti za pojednostavljivanje zadataka koji su u najboljem slučaju svakodnevni, a u najgorem kritično dugotrajni. Možete uštedjeti sate i sate vremena konfigurirajući okruženje novih korisnika i računala koja se pridružuju vašoj domeni pomoću GPO-ova za primjenu standardiziranog, univerzalnog.

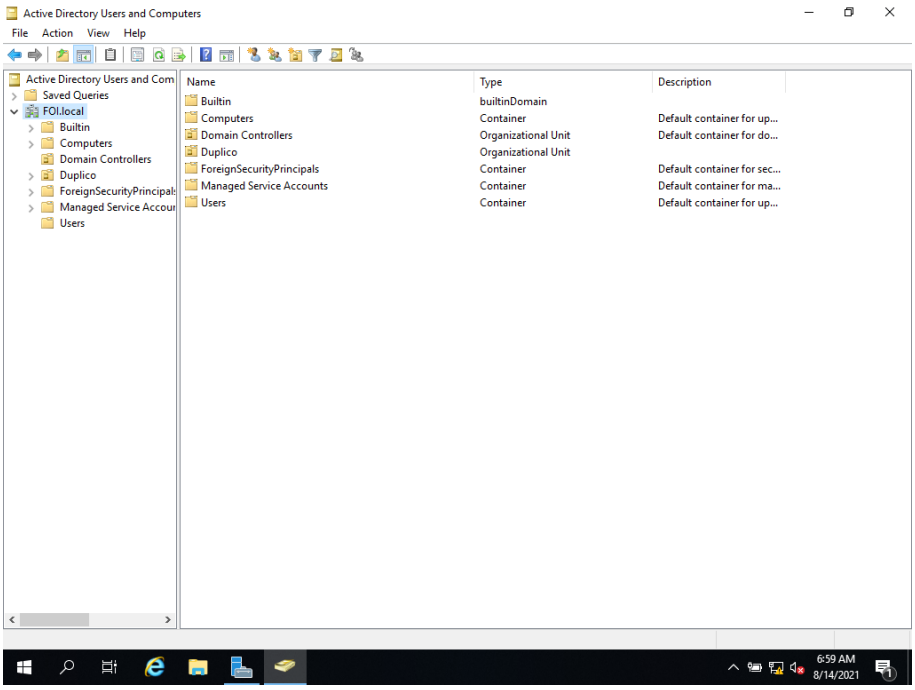
GPO se mogu koristiti za implementaciju ažuriranja softvera i zakrpa sustava kako bi se osiguralo da je vaše okruženje zdravo i ažurirano u skladu s najnovijim sigurnosnim prijetnjama.

4.2 Kreiranje organizacijskih jedinica i korisnika



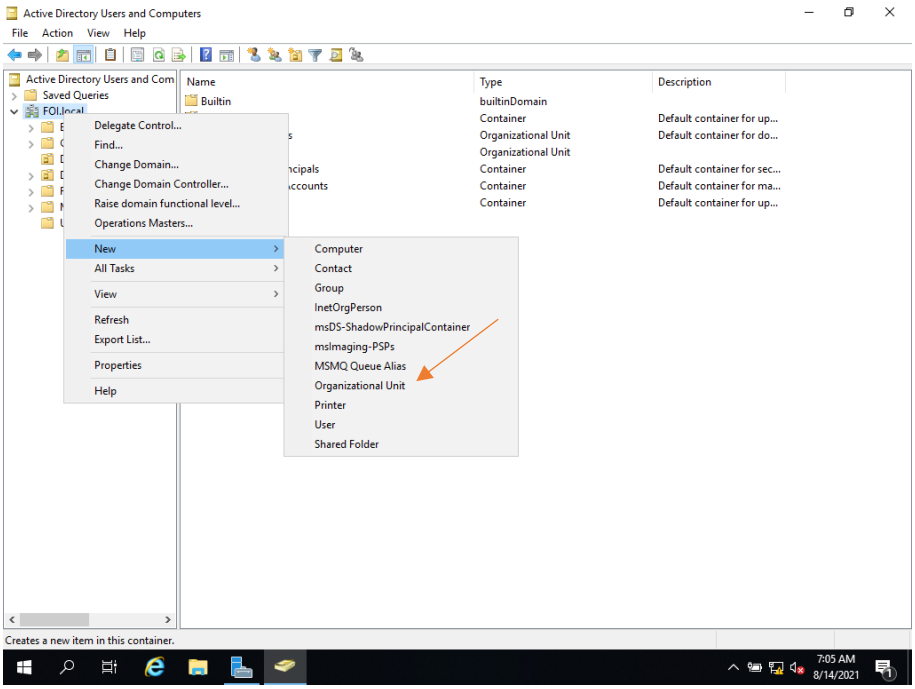
Slika 37 Active Directory korisnici i računala 1

Unutar „Server Managera“ u gornjem desnom kutu odaberemo „Tools“ te „Active Directory Users and Computers“.



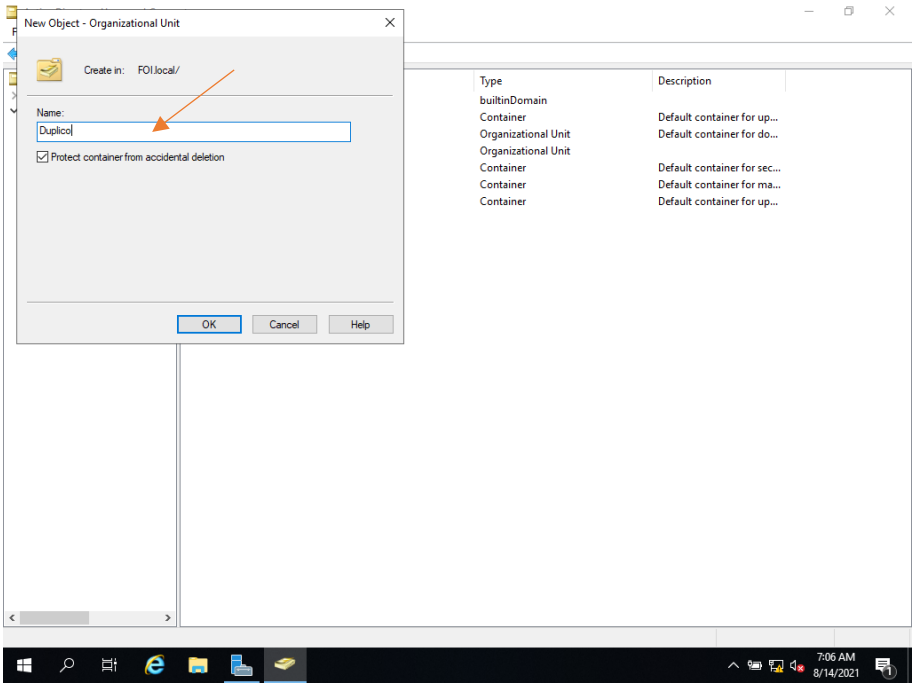
Slika 38 Active Directory korisnici i računala 2

Otvorit će se gore prikazani prozor koji nam prikazuje korisnike, računala te organizacijske jedinice. Osim što ih prikazuje, administrator sustava može upravljati istima, te kreirati nove.



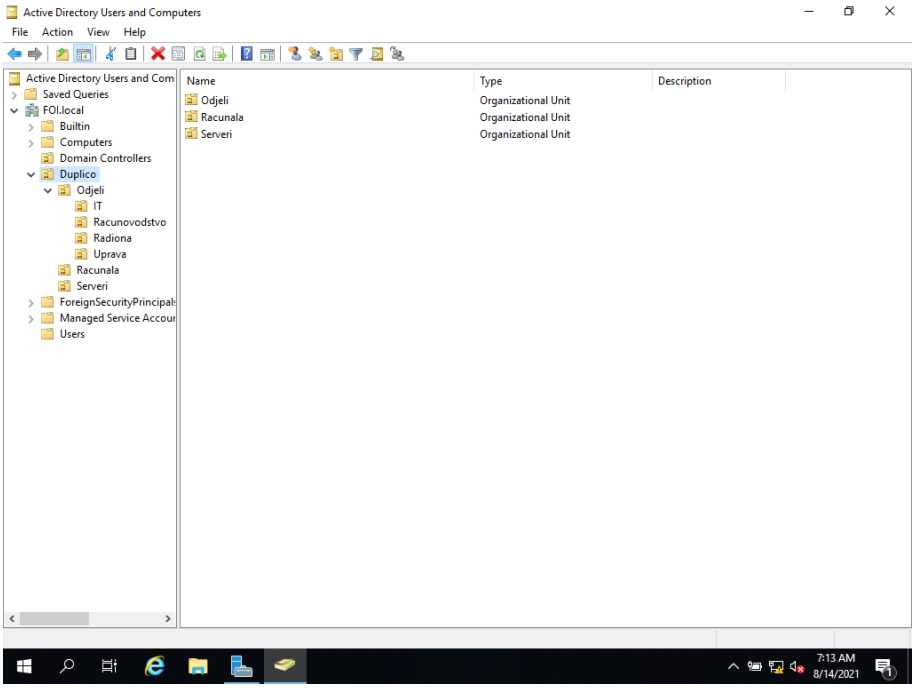
Slika 39 Organizacijska jedinica 1

Desni klik na domenu, „New → Organizational Unit“



Slika 40 Organizacijska jedinica 2

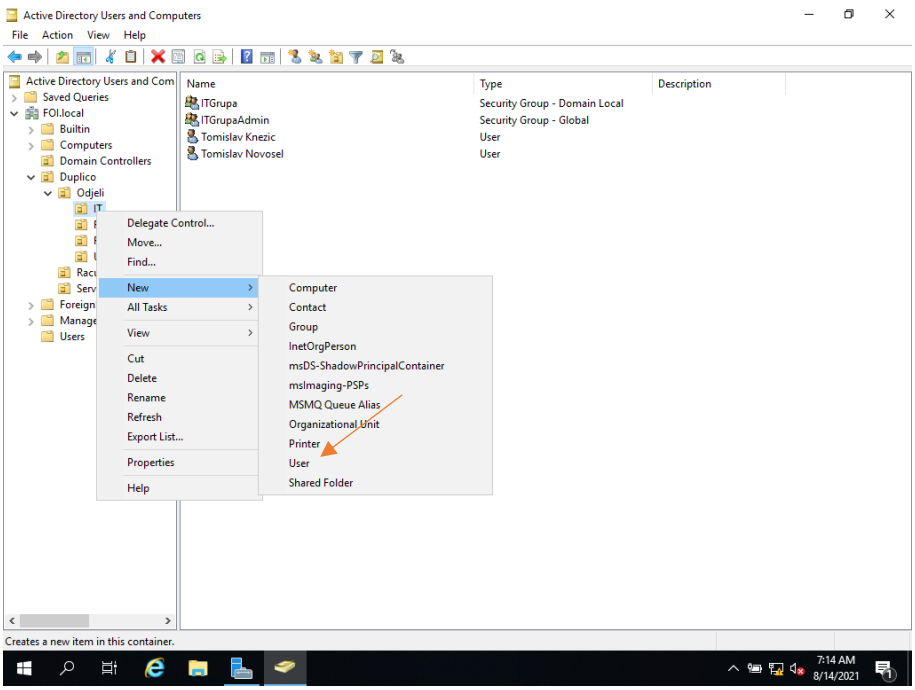
Upišemo naziv organizacijske jedinice, te opcionalno možemo odabrati kvačicu ispod da se ista ne može „slučajno“ obrisati. Iz iskustva, preporučujem odabrati tu kvačicu.



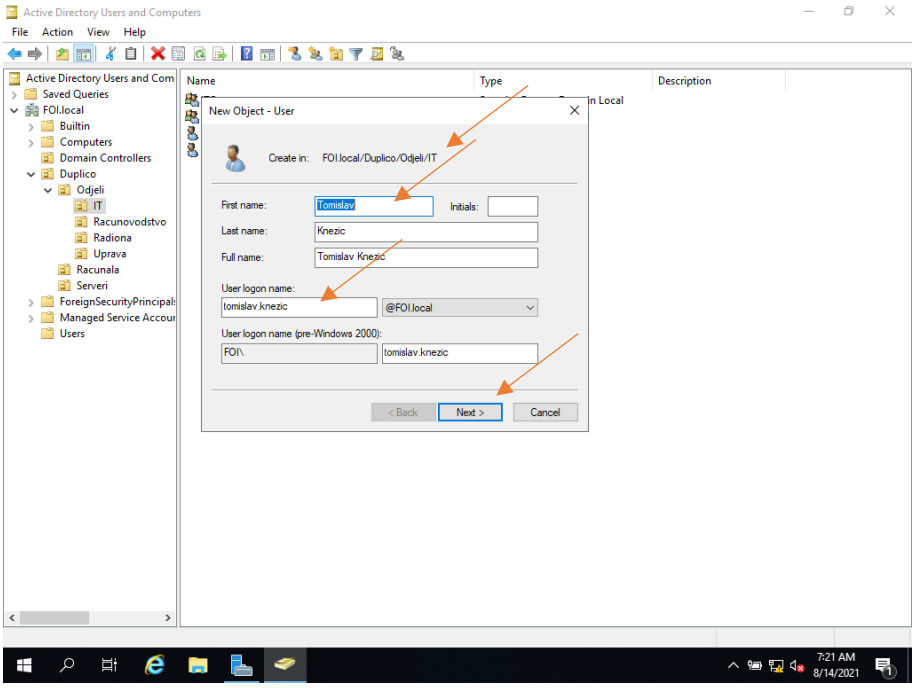
Slika 41 Organizacijska jedinica 3

Na slici iznad vidimo kreirane organizacijske jedinice tvrtke „Duplico d.o.o.“. Iste smo kreirali prema gore navedenim naputcima. U te organizacijske jedinice dodavat ćemo korisnike prema odjelu u kojem rade, a sva računala unutar organizacijske jedinice „Računala“.

Na isti način, kako smo kreirali i organizacijske jedinice, kreiramo i korisnike. Odaberemo željenu organizacijsku jedinicu, desni klik, „New → User“.



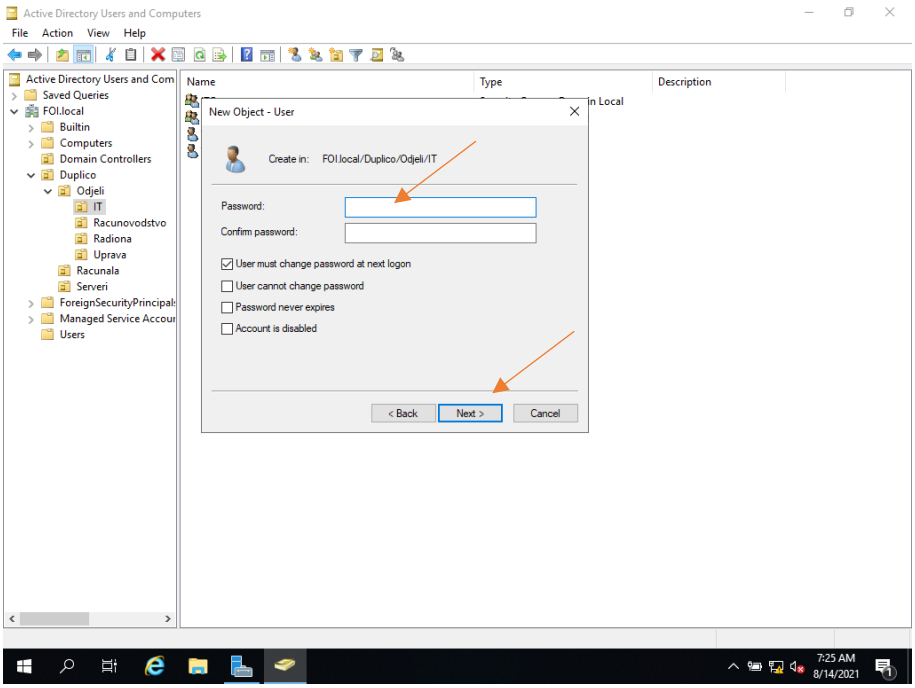
Slika 42 Kreiranje korisnika 1



Slika 43 Kreiranje korisnika 2

Otvorit će se prozor u kojem se jasno vidi putanja gdje će korisnik biti kreiran. Isti se može, naknadno i prema potrebi, premjestiti u drugu organizacijsku jedinicu.

Ovdje upisujemo Ime i Prezime te korisničko ime koje će se koristiti unutar domene te stisnemo „Next“. Npr. Tomislav Knezić ima korisničko ime tomislav.knezic@foi.local.



Slika 44 Korisnička lozinka

Sljedeći prozor koji se pokaže jest prozor za unos lozinke. Ovdje, u globalu, odabiremo da korisnik mora unijeti lozinku prilikom prvog logiranja, a ako to ne želimo, zadamo lozinku, odnosno administrator zadaje lozinku te stavi kvačicu na „Password never expires“.

4.3 Sigurnosne grupe (Security Groups)

Sigurnosne grupe od vitalnog su značaja za održavanje odgovarajućih prava pristupa najosjetljivijim podacima i resursima. Sposobnost grupiranja korisnika za dodjeljivanje razina dopuštenja nevjerojatno je korisna za održavanje sigurnosnih politika.

Na primjer, možete koristiti sigurnosne grupe Active Directory za dodjelu dopuštenja na visokoj razini članovima uprave, ograničenje pristupa pojedinim odjelima. Također možete koristiti sigurnosne grupe za dodjelu dopuštenja niže razine novim korisnicima.

Sigurnosne grupe Active Directory također se mogu mijenjati putem Active Directory portala, gdje se korisnici mogu pomicati ili potpuno ukloniti.

Sigurnosne grupe karakterizira opseg koji identificira u kojoj se mjeri grupa primjenjuje u stablu domene ili šumi. Opseg grupe definira gdje se grupi mogu dodijeliti dopuštenja. Sljedeća tri opsega grupa definiraju Active Directory:

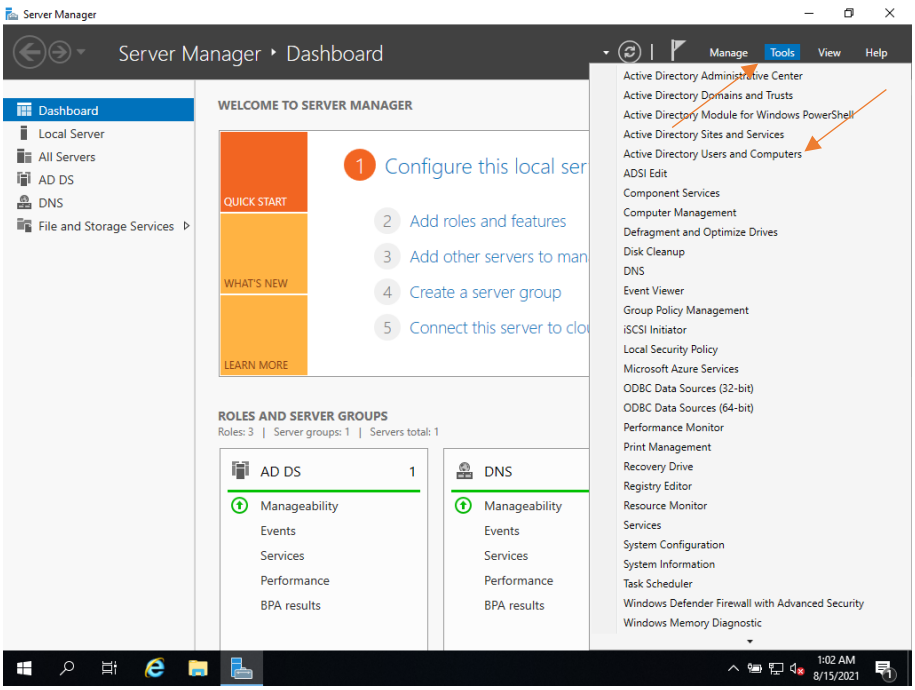
- Univerzalna (universal)
- Globalna (global)
- Lokalna (domain local)

Univerzalna grupa može imati račune s bilo koje domene u istoj šumi, globalne grupe iz bilo koje domene u istoj šumi i ostale univerzalne grupe iz bilo koje domene u istoj šumi. Može se pretvoriti u Domain Local ako grupa nije član nijedne druge univerzalne grupe. Može se pretvoriti u globalnu ako grupa ne sadrži druge univerzalne grupe. Može dati prava na bilo kojoj domeni u istoj šumi ili šumama.

Globalna grupa može imati račune s iste domene, druge globalne grupe iz iste domene. Može se pretvoriti u univerzalnu ako grupa nije član nijedne druge globalne grupe. Može dati prava na bilo kojoj domeni u istoj šumi ili povjerljivim domenama ili šumama.

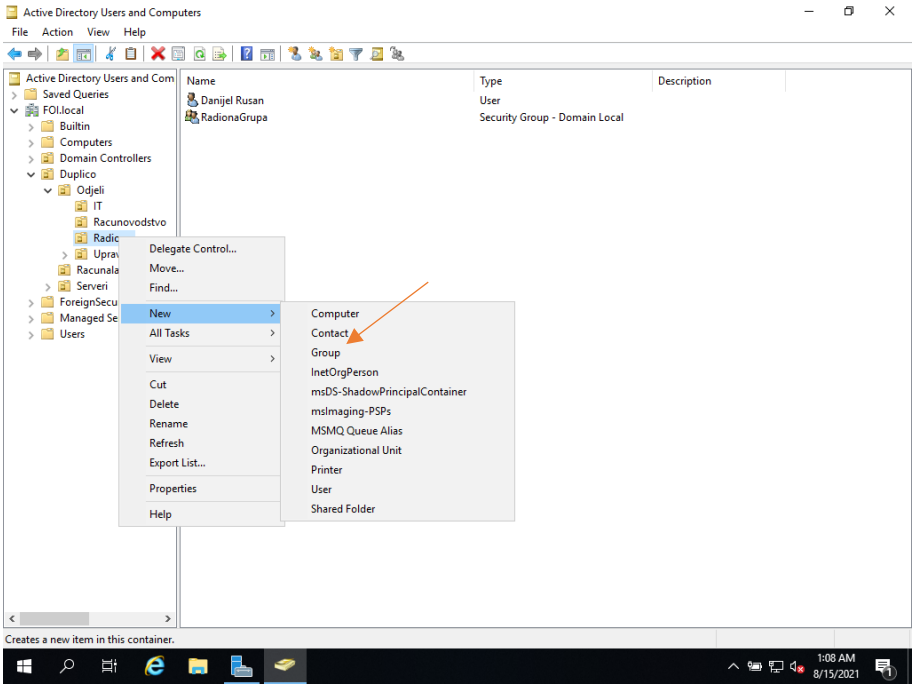
Lokalna grupa može imati račune s bilo koje domene ili bilo koje pouzdane domene, globalne grupe iz bilo koje domene ili bilo koje pouzdane domene, univerzalne grupe iz bilo koje domene u istoj šumi i ostale domene lokalne grupe iz iste domene. Može se pretvoriti u univerzalnu ako grupa ne sadrži druge lokalne grupe domene. Može dati prava unutar iste domene.

4.3.1 Kreiranje sigurnosne grupe



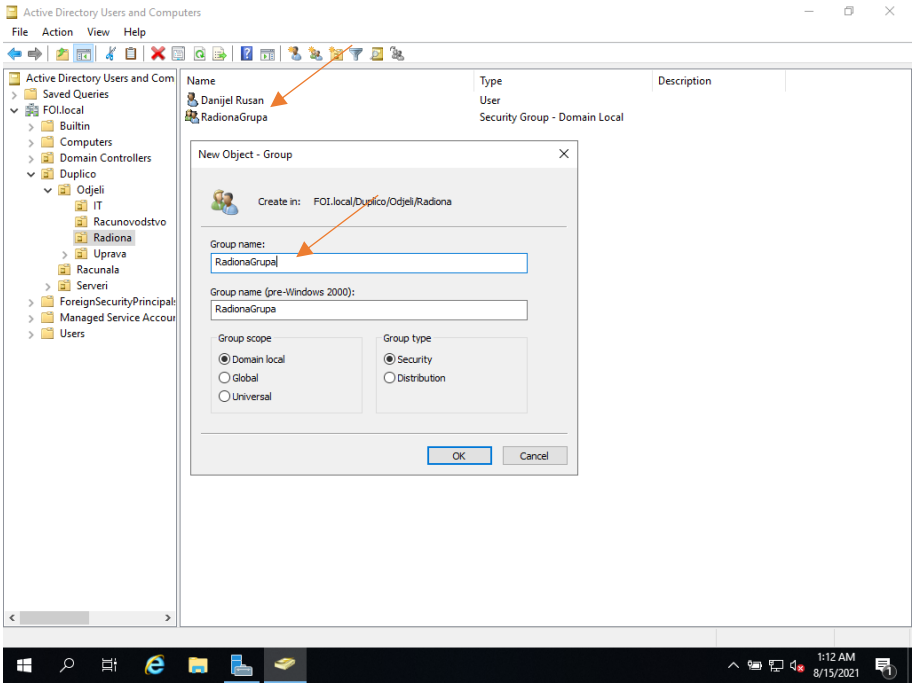
Slika 45 Sigurnosne grupe 1

Unutar „Server Managera“ odaberemo „Tools“ i „Active Directory Users and Computers“.



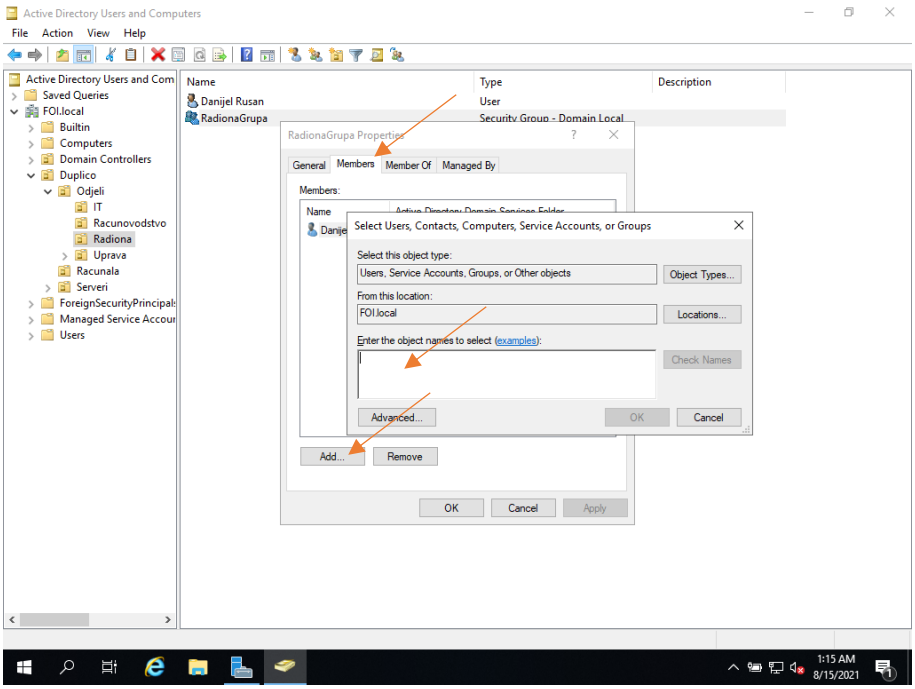
Slika 46 Sigurnosne grupe 2

U prošlom poglavju (4.2) prikazali smo kako se kreiraju organizacijske grupe i korisnici. Navigiramo se prema željenoj organizacijskoj grupi, npr. „Radiona“, te desnim klikom miša kliknemo na nju, New → Group.



Slika 47 Sigurnosne grupe 3

Otvorit će se prozor „New Object – Group“. U „Group name“ napišemo željeno ime sigurnosne grupe, npr. „RadionaGrupa“, te odaberemo vrstu grupe, tzv. scope, što smo malo prije objasnili. U ovom slučaju, odabrat ćemo „Domain local“ i „Security“. Potvrdimo sa OK.

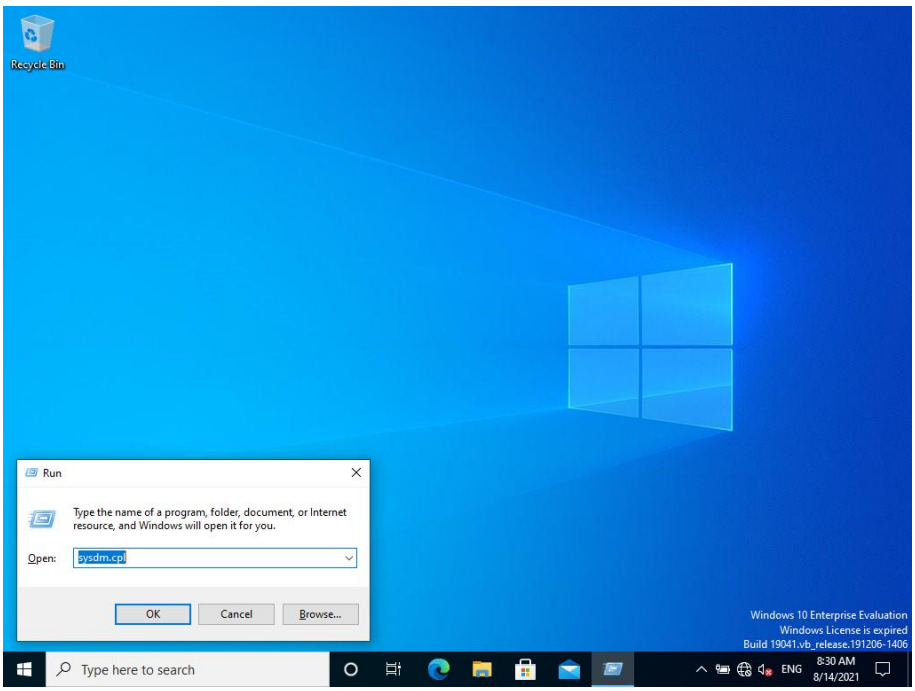


Slika 48 Sigurnosne grupe i dodavanje korisnika

Da bi sigurnosna grupa „imala smisla“, moramo istoj pridružiti korisnike. To se radi na način da dvoklikom stisnemo na željenu grupu, navigiramo se na tab „Members“ i pritisnemo tipku „Add“. Otvorit će se prozorčić, slika 48, te upišemo željenog korisnika i potvrdimo sa OK! Korisnik je dodan u sigurnosnu grupu.

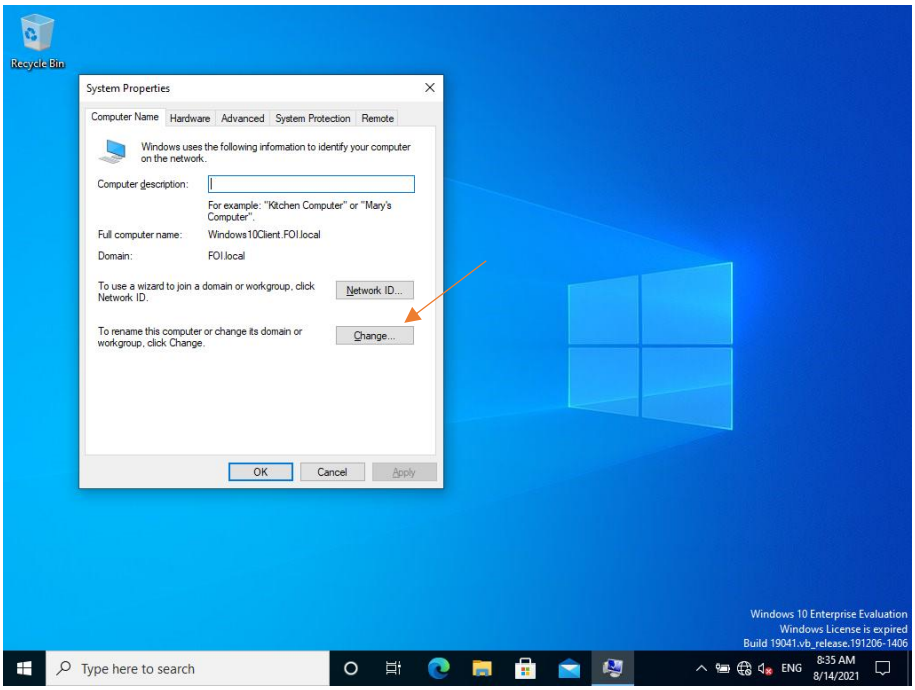
4.4 Dodavanje računala (klijenta) u Active Directory

U sljedećih par koraka prikazat ćemo kako se računalo dodaje u domenu, odnosno Active Directory. Podrazumijeva se da je računalo unutar iste lokalne mreže kao i domain controller.



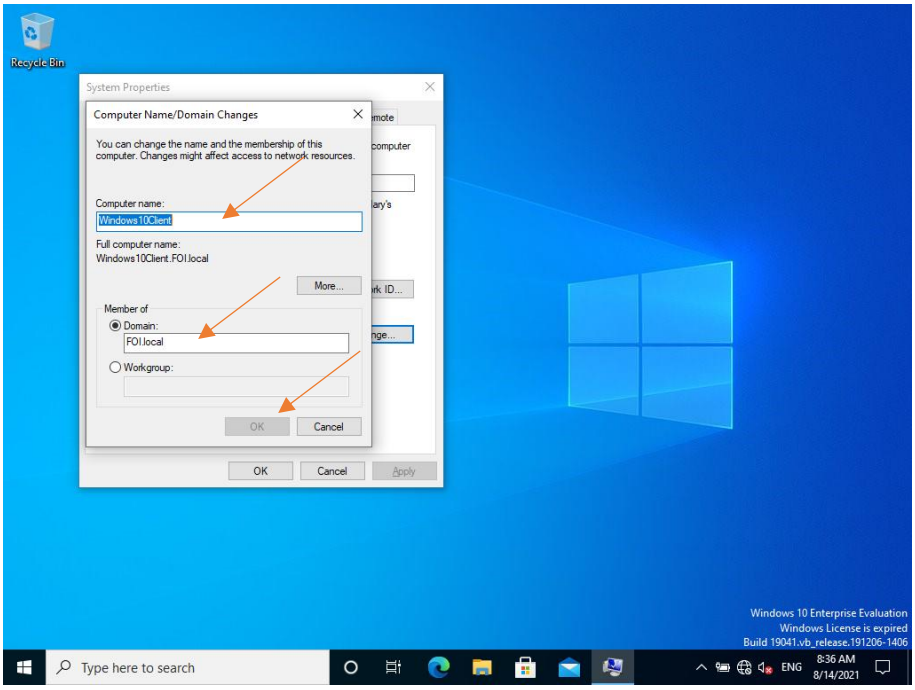
Slika 49 Postavke sistema 1

Na klijentskom računalu, odnosno računalu kojeg želimo dodati u domenu, pokrenemo Run prozorčić (Search → Run ili prečac Windows tipka + R) te utipkamo „sysdm.cpl“. Otvorit će se prozor „System Properties“.



Slika 50 Postavke sistema 2

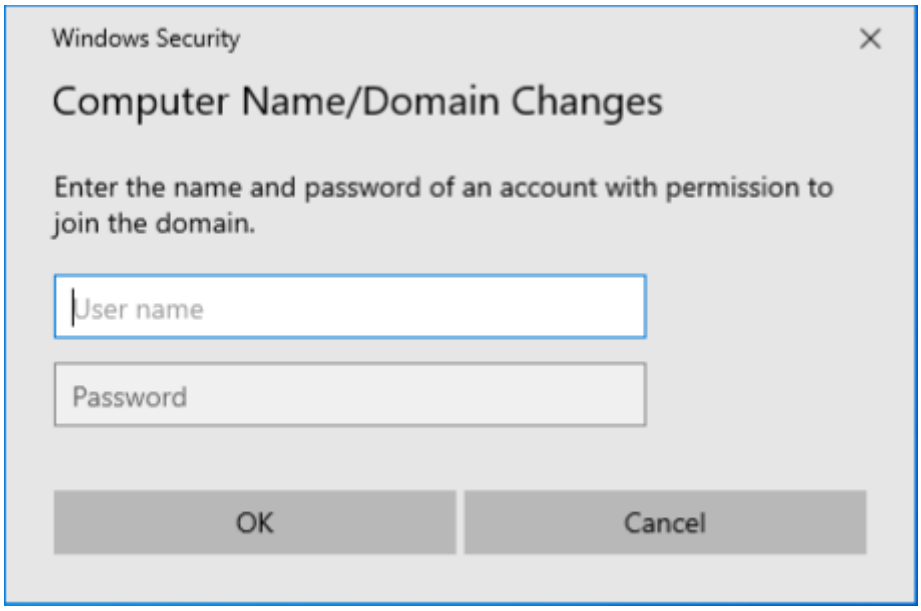
Ovdje odaberemo „Change“ kako je prikazano na slici.



Slika 51 Član domene

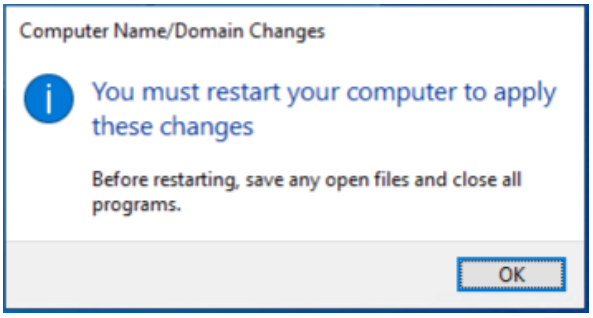
Ako želimo promijeniti „Ime računala“, upisujemo naziv po želji. Ovdje na slici je to Windows10Client, a možemo staviti i prema odjelu, npr. Radiona01 i slično.

Pod poljem „Member of“ upisujemo naziv domene i potvrdimo sa OK. O tome smo već pisali pod poglavljem Active Directory.



Slika 52 Administratorska lozinka

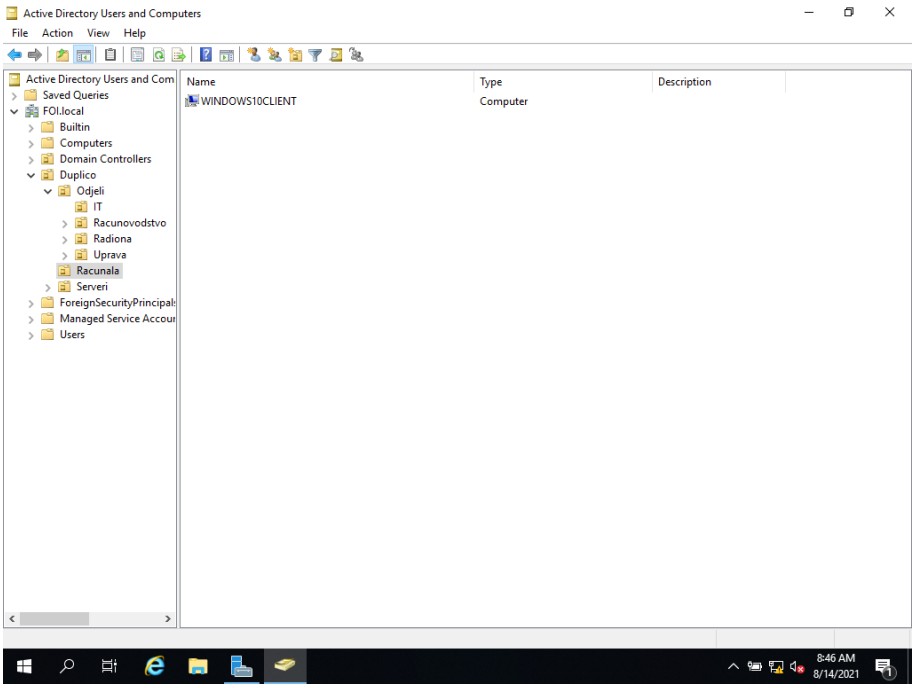
Pritiskom na tipku OK, otvorit će se dijaloški prozor u kojem upisujemo korisničko ime i lozinku domenskog administratora.



Slika 53 Ponovno pokretanje sistema

Ako je sve prošlo u redu, dobit ćemo poruku „Welcome to the foi.local domain“, stisnemo OK i sustav će nas tražiti da ponovno pokrenemo računalo, tzv. restart.

Kada se računalo ponovno pokrene, član je domene, te se logiramo sa svojim domenskim korisničkim imenom i lozinkom koju smo dobili od administratora sustava.

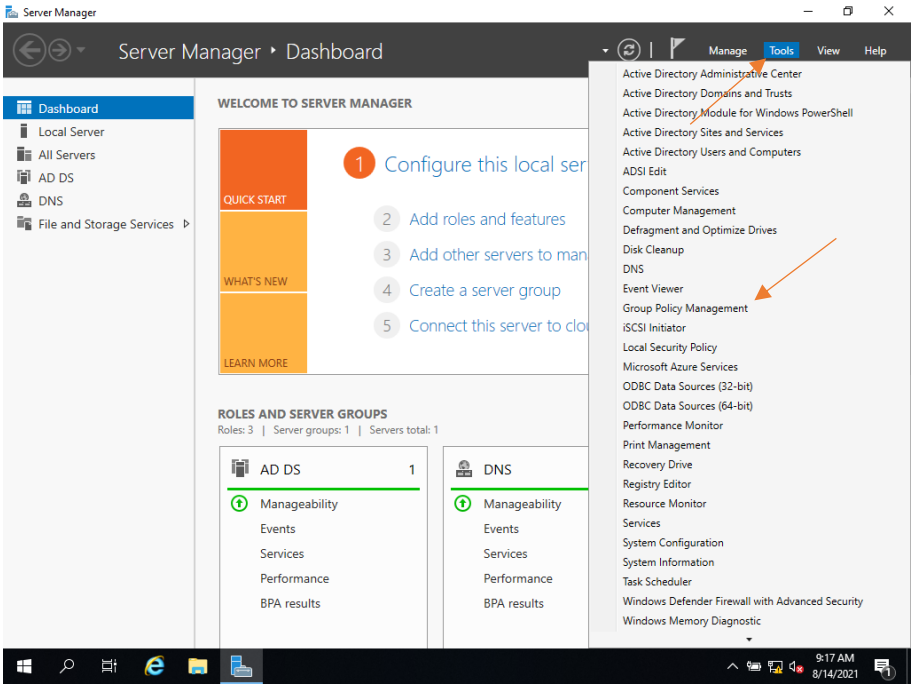


Slika 54 Active Directory računala

Na poslužitelju vidimo da je računalo dodano u Active Directory i administrator ga je već premjestio u odgovarajući odjel.

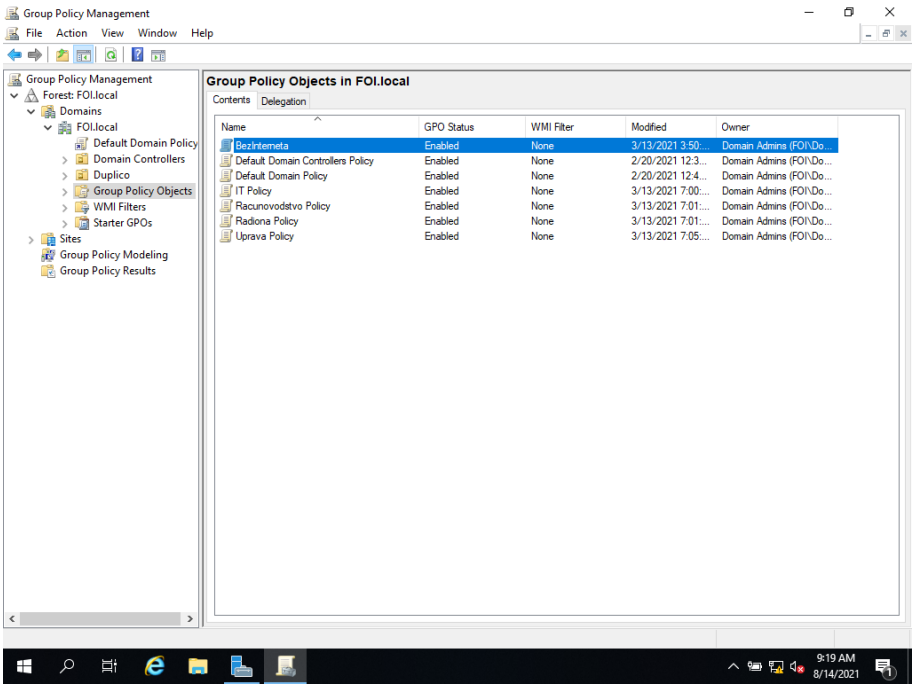
4.5 Kreiranje Group Policy Objects

Ono što još trebamo učiniti, sada kada smo naučili kako kreirati organizacijske jedinice, korisnike te dodati računala u domenu jest kreiranje i implementacija sigurnosnih pravila, koja će pojedine organizacijske grupe, odnosno fizičke odjele unutar poduzeća, na neki način kontrolirati i onemogućiti da pristupaju određenim servisima, procesima i slično, sve prema unaprijed definiranim sigurnosnim pravilima.



Slika 55 Group Policy Management 1

Za pristup Group Policy Objects, unutar Server Managera odaberemo „Tools → Group Policy Management.“

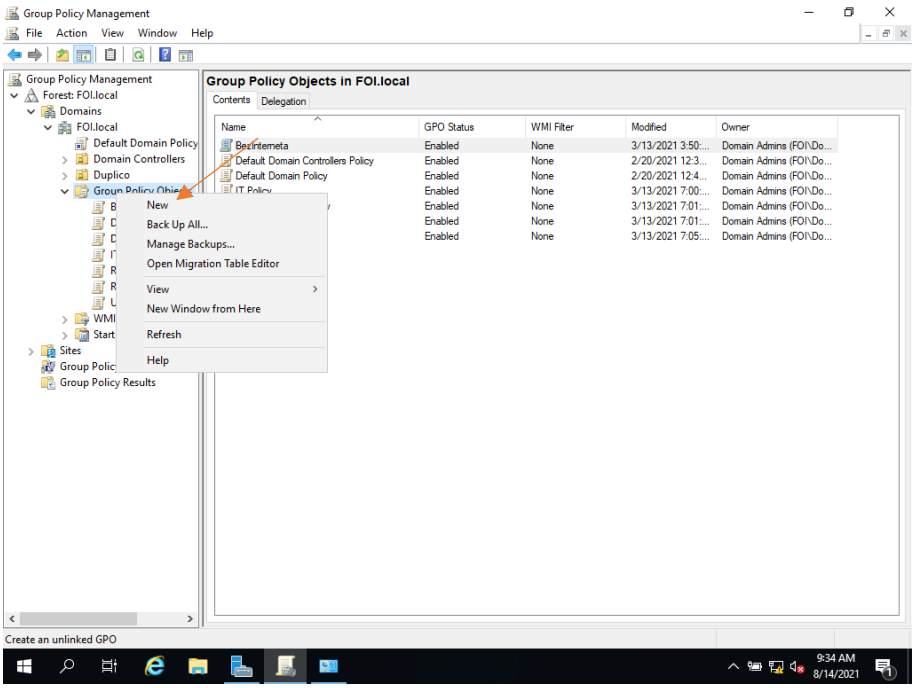


Slika 56 Group Policy Management 2

Otvorit će se prozor kao na slici 56, te vidimo da već imamo definirane neke politike koje su implementirane, odnosno povezano na određene odjele.

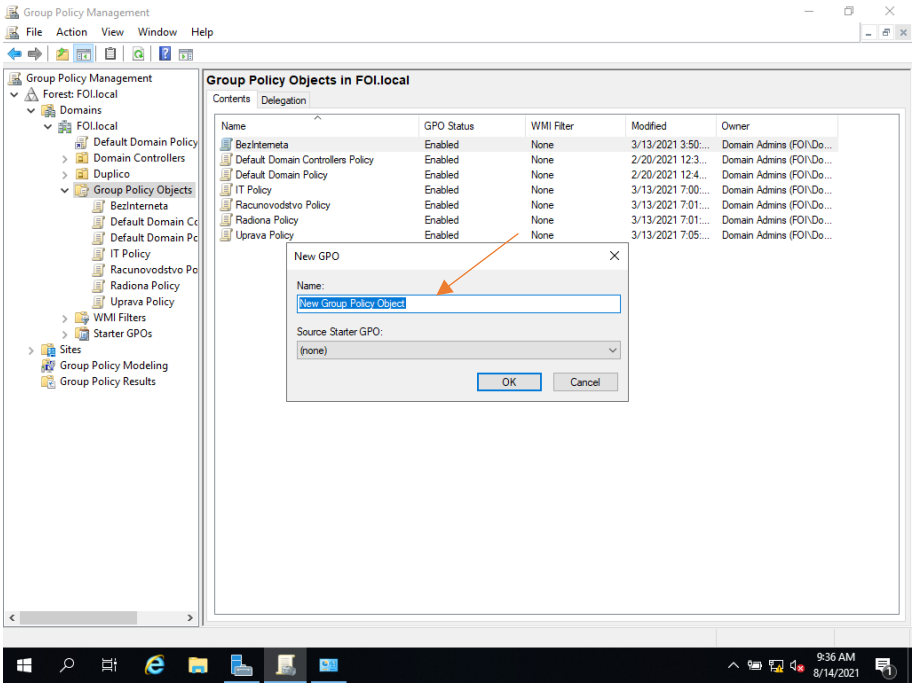
Uzmimo za primjer odjel „Radiona“. U „Radioni“ želimo kreirati i primijeniti sljedeće politike:

- Mapirana mapa RadionaShare
- Share RadionaPrinter
- Notepad.exe se podiže kod logona



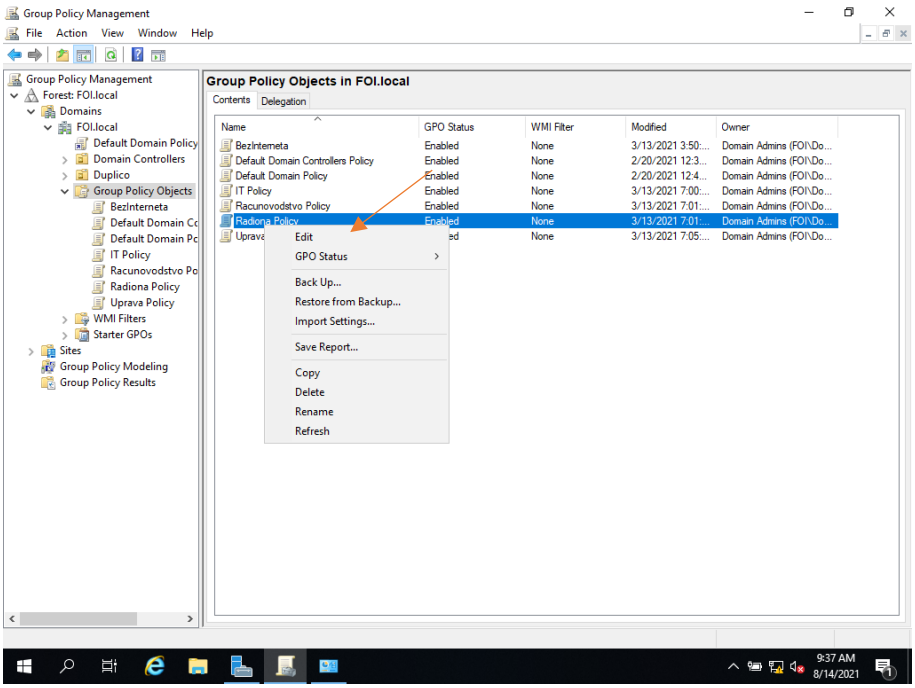
Slika 57 Novi Group Policy objekt 1

Desnim klikom pritisnuti na Group Policy Objects i odabrati „New“.



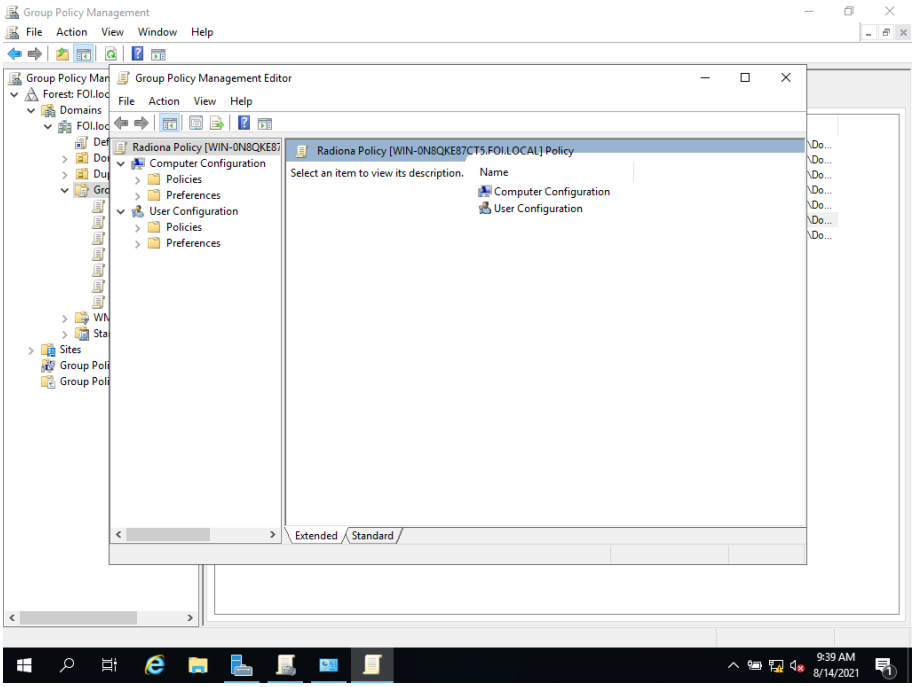
Slika 58 Novi Group Policy objekt 2

Upisati naziv, npr. Radiona Policy te stisnuti OK.



Slika 59 Uredi Group Policy Object 1

Na kreirani profil Radiona Policy stisnuti desnim klikom miša te odabrati „Edit“.



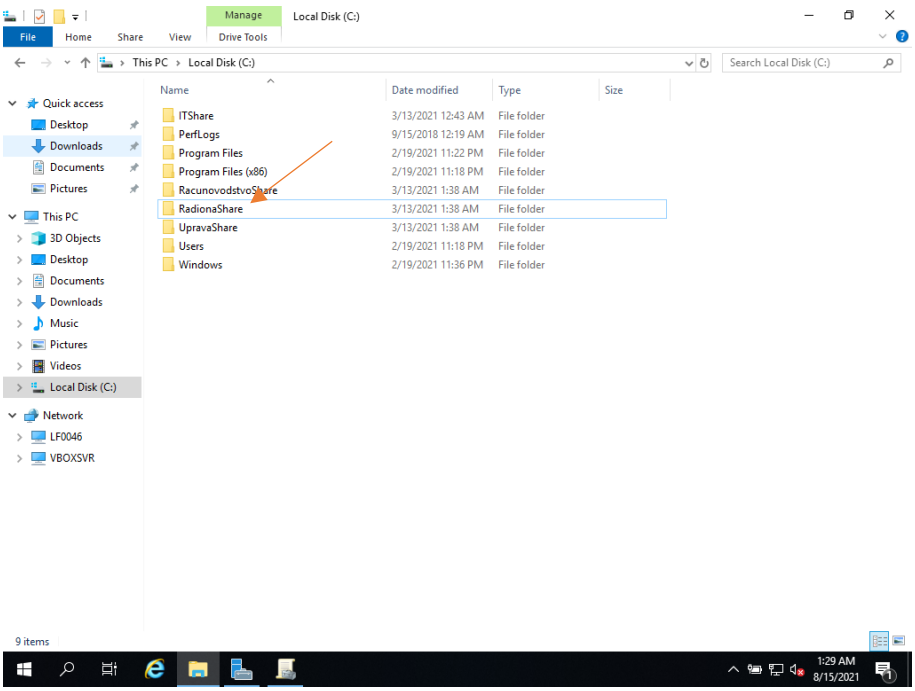
Slika 60 Uredi Group Policy Object 2

Otvorit će se „Group Policy Management Editor“ preko kojeg možemo kreirati sve gore navedene politike.

4.5.1 Mapiranje mape (foldera)

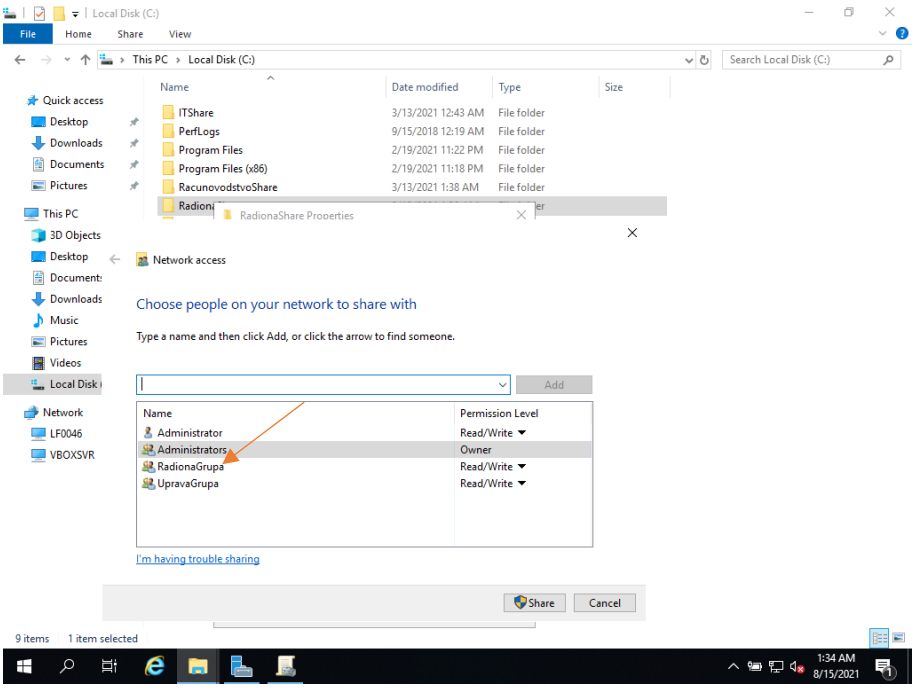
Prva od četiri politike koje ćemo objasniti je mapiranje mrežne mape, odnosno mrežnog pogona. To će se napraviti automatski prilikom prijave korisnika na svoje klijentsko računalo, koje je na domeni.

Otvorimo Windows Explorer i kreiramo željenu mapu na tvrdom disku.



Slika 61 Kreiranje mape

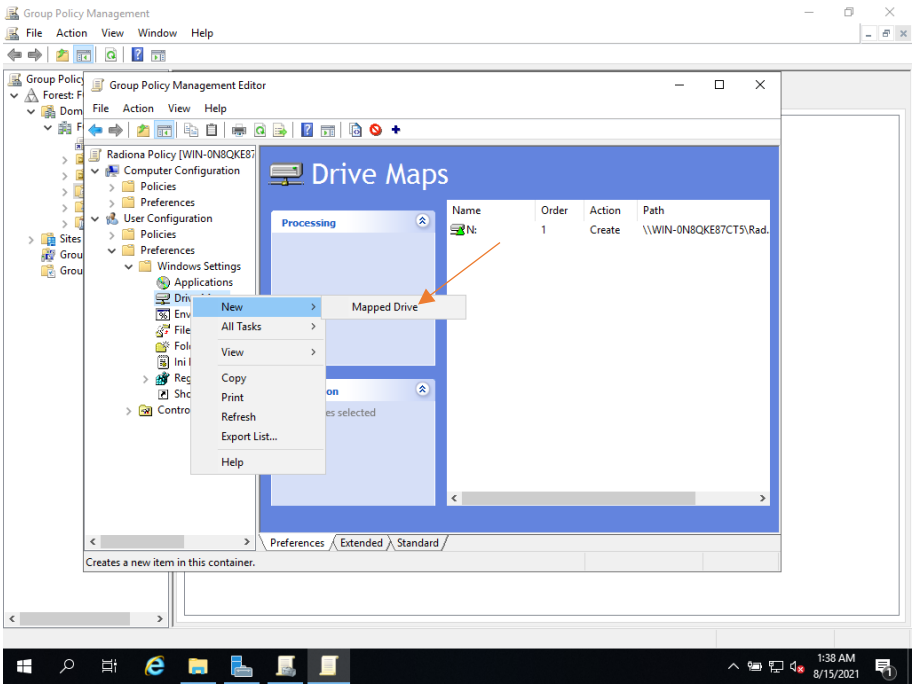
Na slici se vidi da smo kreirali mapu „RadionaShare“. Istoj još moramo omogućiti dijeljenje (share). Desnim klikom kliknemo na navedenu mapu, odaberemo „Properties“ te unutar tog prozora, odaberemo „Share“. Kliknemo na „Share…“, te upišemo željene sigurnosne grupe kojima ćemo omogućiti pristup toj mapi. Ta mapa koristit će se kao mapa u kojoj će se dijeliti resursi i informacije koji su potrebni za svakodnevni rad tog odjela.



Slika 62 Dijeljenje mape

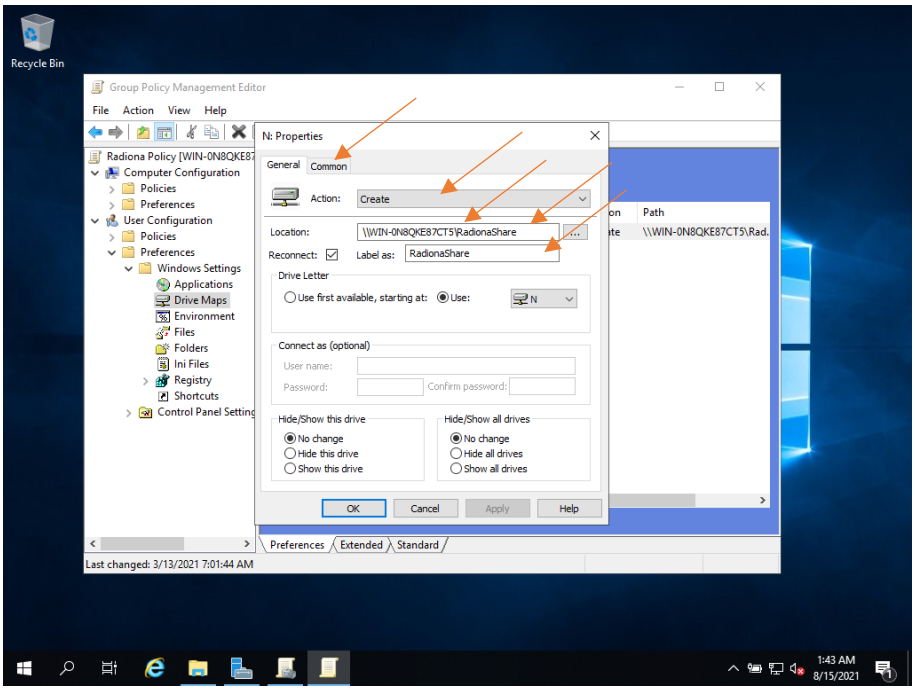
Na slici vidimo da je „RadionaGrupa“ dodana u dijeljenje te smo istoj omogućili čitanje i zapisivanje („Read/Write“). Potvrdimo sa tipkom „Share“.

Sada se vraćamo na „Group Policy Management Editor“ (slika).



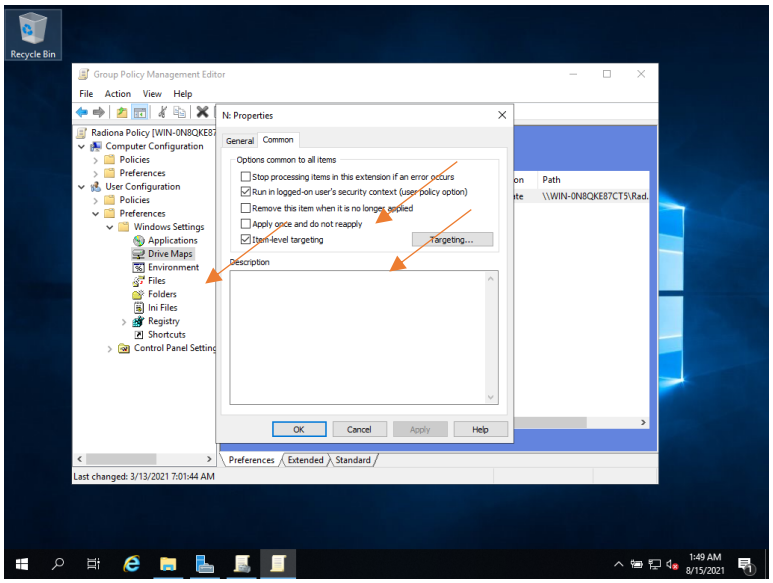
Slika 63 Mapiranje mrežnog pogona 1

Pod „User Configuration → Preferences → Windows Settings“ desnim klikom miša kliknemo na „Drive Maps“ te odaberemo „New → Mapped Drive“.



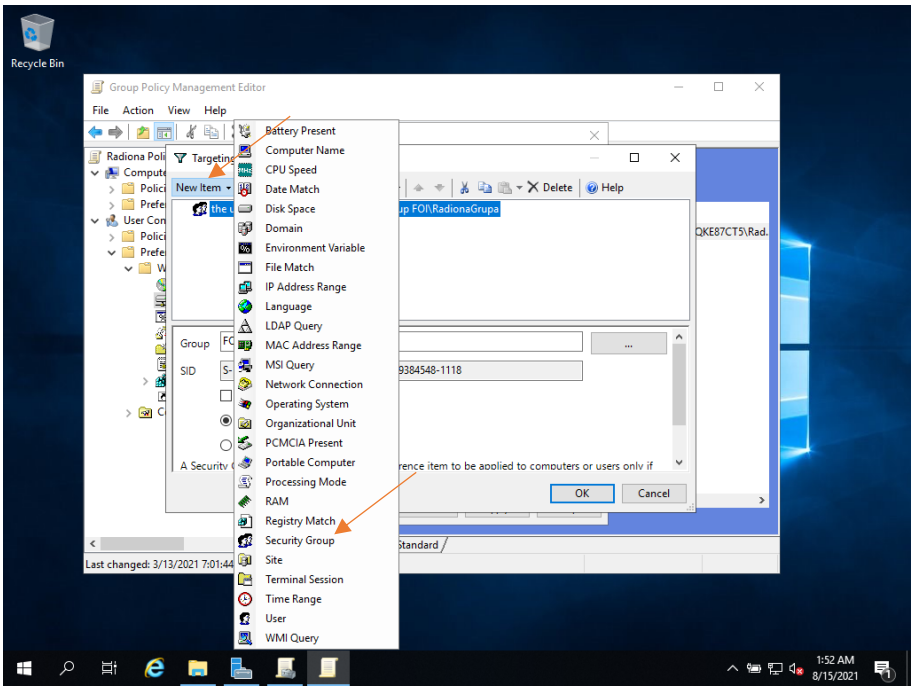
Slika 64 Mapiranje mrežnog pogona opcije 2

Pod „Action“ odaberemo „Create“. U polje lokacija upisujemo mrežnu putanju mape koju želimo mapirati. Sjetite se, kada smo uključili dijeljenje mape (share), dobili smo i mrežnu putanju. U našem slučaju ona izgleda ovako: \\WIN-0N8QKE87CT5\RadionaShare . Stavimo kvačicu na „Reconnect“ te pod Label upišemo ime koje će se pojaviti kao ime dijeljene mape na klijentskom računalu. Na ovom prozoru ostaju još odabrati „Drive Letter“, tipično se to stavlja kao „Z:“, no, može se prema želji. Nakon toga kliknemo na tab „Common“.



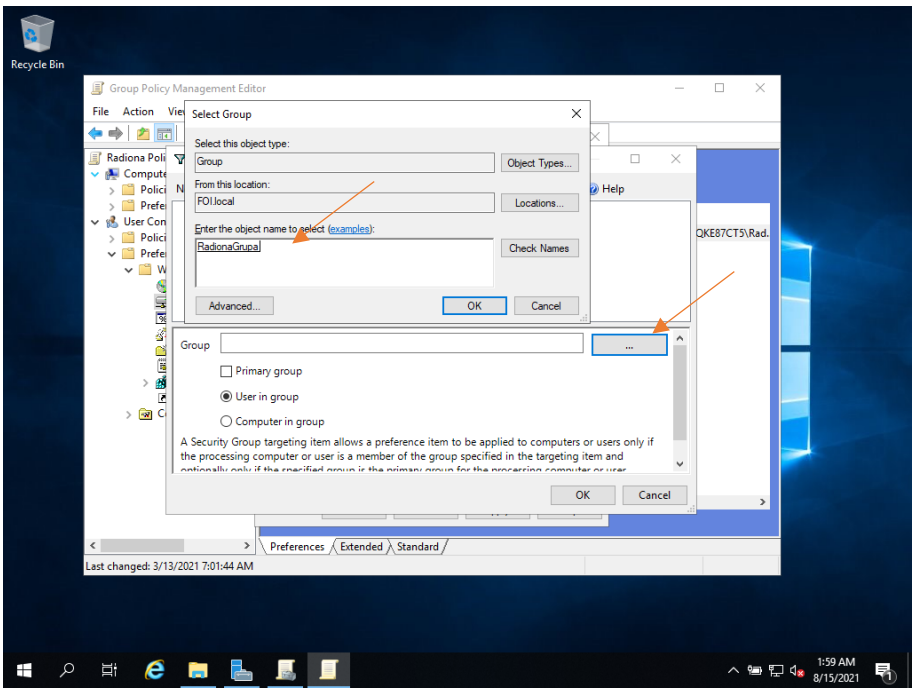
Slika 65 Mapiranje mrežnog pogona opcije 3

Ovo je vrlo bitan prozor i preko njega sve dosada prikazano i naučeno ustvari pridružujemo određenim sigurnosnim grupama ili pojedinim korisnicima i slično. Znači, stavimo kvačicu na „Run in logged-on user's security option“ te obavezno „Item-level targeting“ i stisnemo na tipku „Targeting…“.



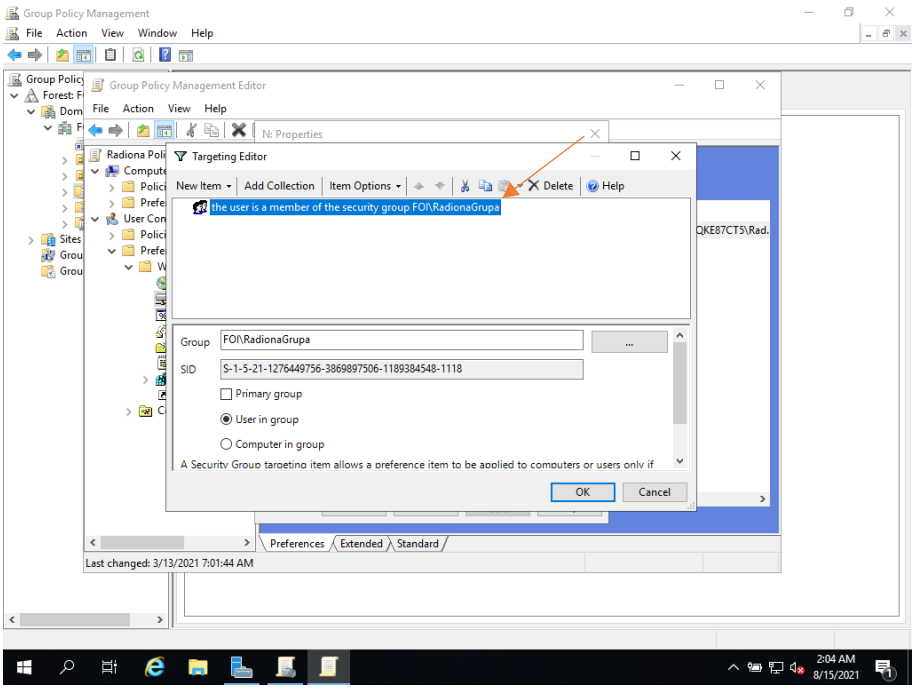
Slika 66 Dodaj sigurnosnu grupu 1

Otvorit će se prozor „Targeting Editor“. Odaberemo „New Item“ i „Security Group“.



Slika 67 Dodaj sigurnosnu grupu 2

Kada smo otvorili „New Item → Security Group“ stisnemo na „…“ (tri točkice) te se otvorit prozorčić „Select Group“, upišemo npr. „RadionaGrupa“, stisnemo „Check Names“ te potvrdimo sa „OK“.

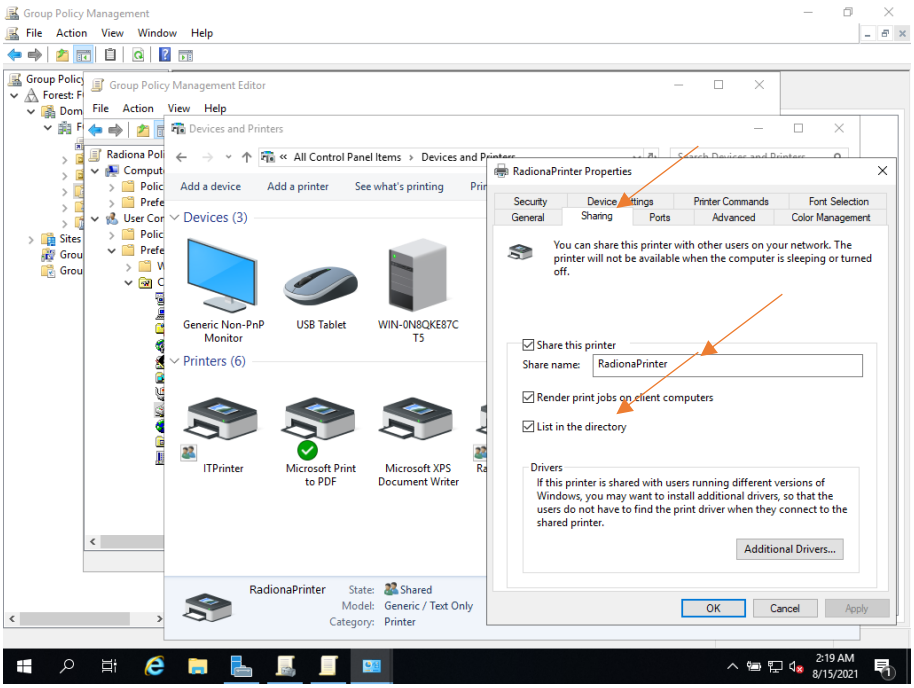


Slika 68 Dodaj sigurnosnu grupu 3

Ovako izgleda završeno podešavanje navedene sigurnosne politike. Potvrdimo svaki prozorčić sa „OK“ i vratimo se na „Group Policy Management Editor“.

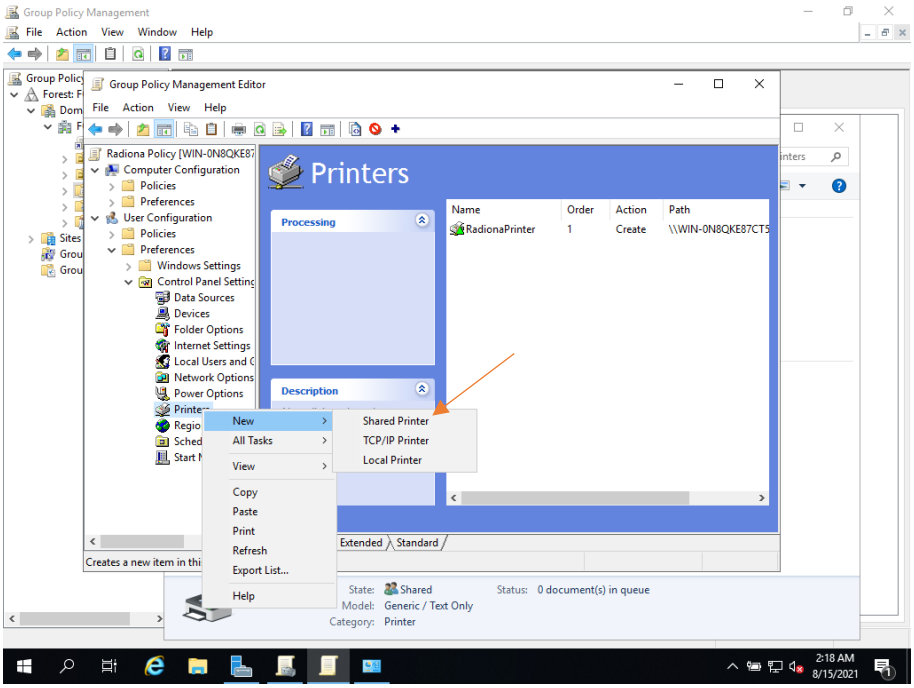
4.5.2 Dijeljeni pisač (printer)

Vrlo slična logika stoji i iza dijeljenja pisača. Pisači su instalirani na serveru te je omogućeno njihovo dijeljenje. Sve ostale postavke podešavamo preko „Group Policy Management Editor-a“. Kreiramo profil podijeljenog pisača, pridružimo tom profilu pisač, te pod „Item level targeting“ odabaremo sigurnosnu grupu kojoj želimo pridružiti taj profil. Kroz sljedećih par slika ćemo prikazati kako se to radi.



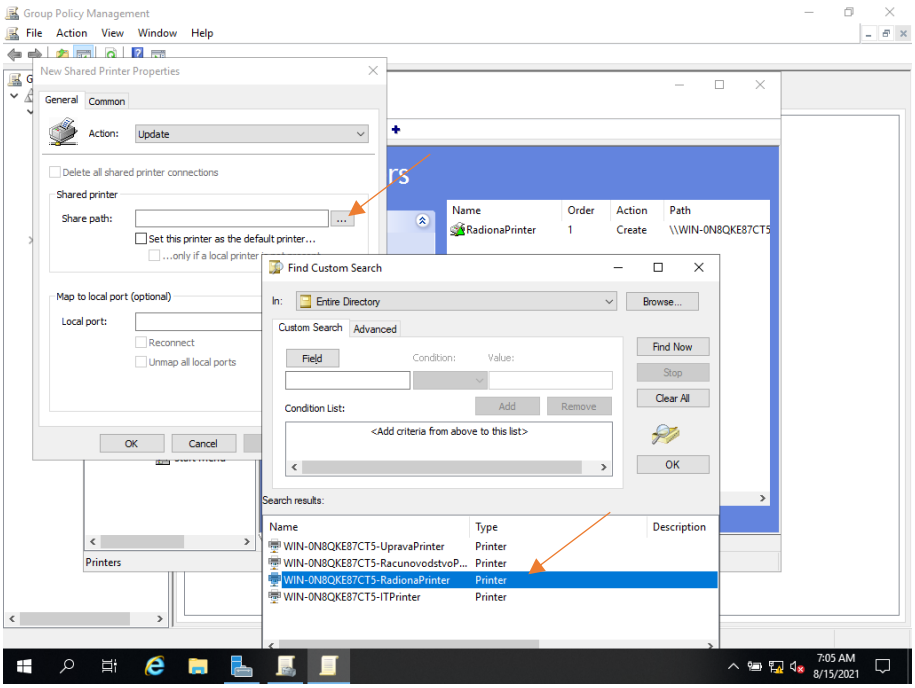
Slika 69 Dijeljeni pisač

U „Upravljačkoj ploči“ („Control panel“) provjerimo dali imamo instalirane sve pisače koje želimo dijeliti. Odaberemo željeni pisač te pod „Sharing“ podijelimo isti. Vratimo se na „Group Policy Management Editor“.



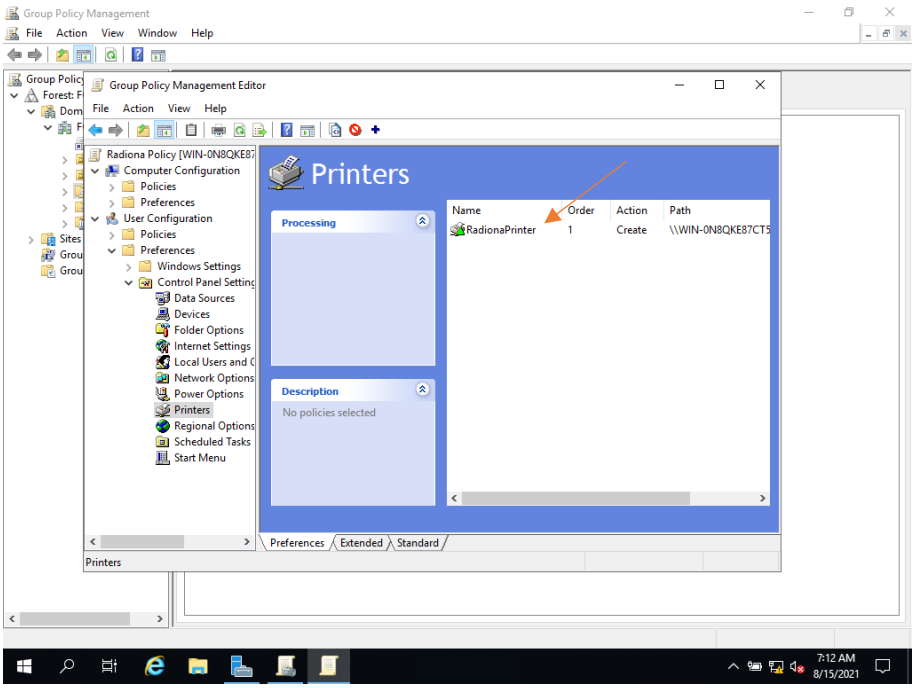
Slika 70 Dijeljeni pisač

Navigiramo se pod „User Configuration → Preferences → Control panel settings“. Desnim klikom miša na „Printers“ odaberemo „New → Shared Printer“.



Slika 71 Group Policy printer

Na slici 71 vidimo da se otvori prozor „New Shared Printer Properties“ na kojem odaberemo pod tipku „…“ (tri točkice). U novom prozoru „Find Custom Search“ odaberemo željeni dijeljeni pisač, u našem slučaju „RadionaPrinter“ i potvrdimo sa OK.

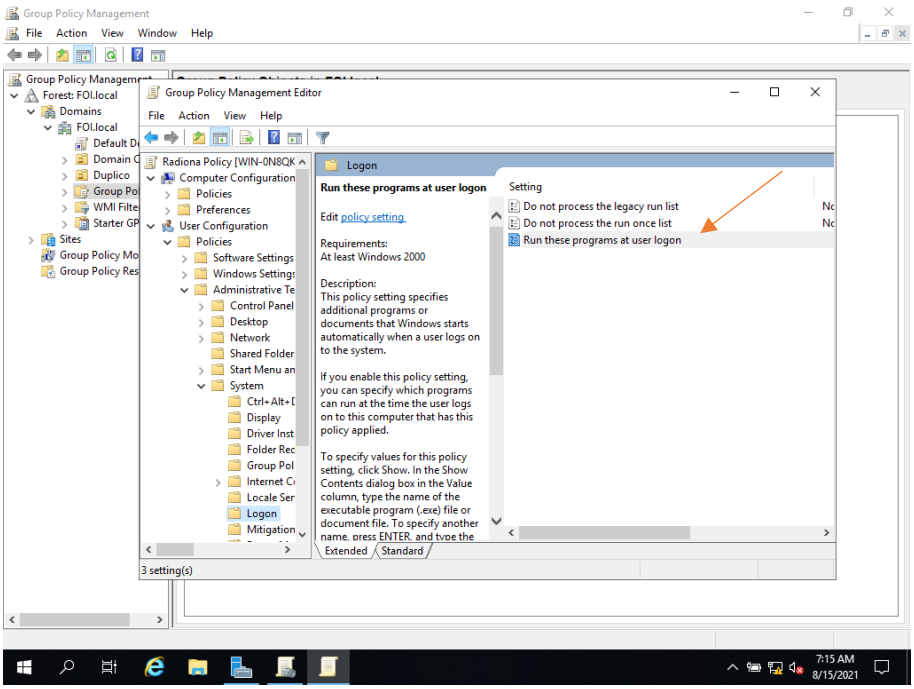


Slika 72 Group Policy printer

Pisač je uspješno dodan u naš policy.

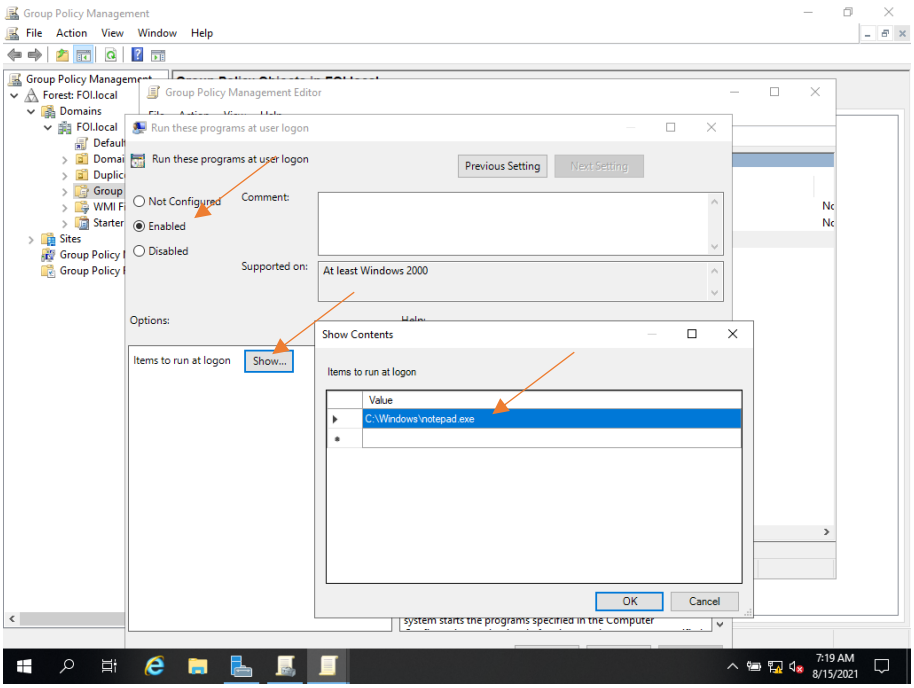
4.5.3 Automatsko pokretanje programa

Zadnje što je još ostalo prikazati jest kako namjestiti da se prilikom prijave u sustav automatski pokrene program. To se može namjestiti za bilo koju grupu, korisnika i slično. Odabrali smo program „Notepad.exe“.



Slika 73 Pokretanje programa

Unutar „Group Policy Managementa“, pod „User Configuration → Policies → Administrative Templates → System → Logon“ odaberemo opciju „Run these programs at user logon“.



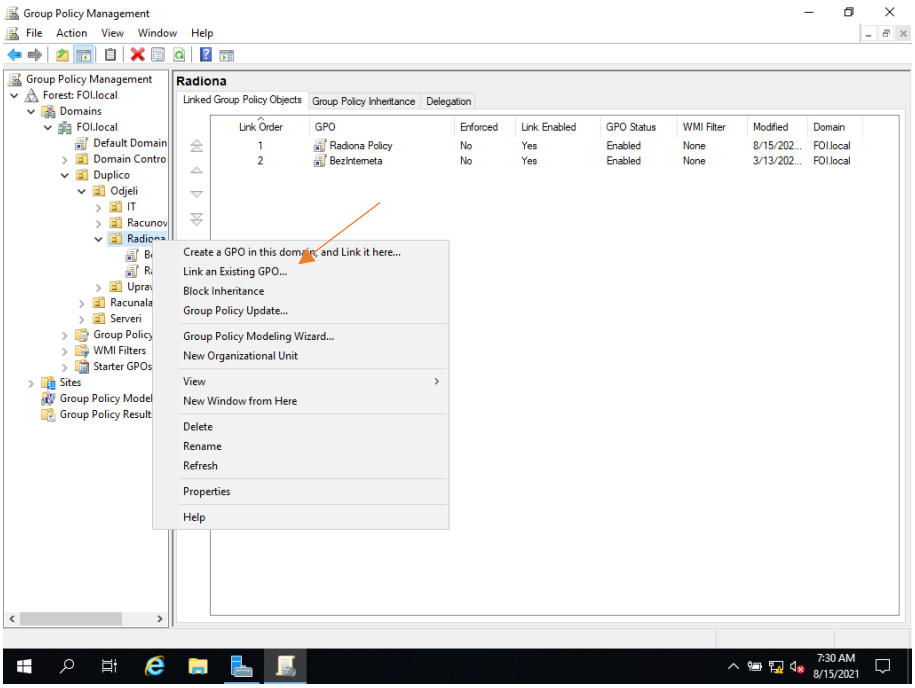
Slika 74 Pokretanje programa

Na slici 74 vidimo da se otvorio novi prozor na kojem odaberemo točkicu „Enabled“ te stisnemo tipku „Show“ odmah pored teksta „Items to run at logon“. Otvorit će se novi prozorčić u kojem navigiramo prema aplikaciji koju želimo pokrenuti, u našem slučaju „Notepad.exe“. Potvrdimo sa OK.

4.6 Primjena izrađenih Group policy objecta

Prikazali smo kako mapirati mapu i dodijeliti je određeno sigurnosnoj grupi. Prikazali smo kako podijeliti pisač te kako namjestiti da se prilikom prijave određenog korisnika ili korisnika koji pripada određenoj sigurnosnoj grupi automatski pokrene program kod prijave u sustav.

No, nešto još fali. Znači, sve gore navedeno „ugradili“ smo u profil Group Policy Objecta kojeg smo nazvali „Radiona Policy“. Isti taj profil moramo još pridružiti organizacijskoj grupi unutar Active Directory-a.



Slika 75 Primjena GPO

U „Group Policy Management“ prozoru, navigiramo se, odnosno namjestimo se na organizacijsku grupu kojoj želimo dodijeliti sigurnosnu politiku, odnosno GPO koji smo kreirali. Desnim klikom pritisnemo na organizacijsku grupu te odaberemo „Link an Existing GPO“. Odabaremo profil koji želimo i pritisnemo OK.

Isti taj GPO sada je dodijeljen organizacijskoj grupi te će se primjenjivati na sve korisnike koji se nalaze unutar te organizacijske grupe. Organizacijska grupa može imati pridruženo puno više od samo jednog GPO-a.

5. Zaključak

Cilj ovog završnog rada bio je prikazati instalaciju i implementaciju sigurnosnih politika unutar Active Directory-a. Rad se sastoji od Windows Server 2019 operacijskog sustava i Windows 10 operacijskog sustava. Oba sustava instalirana su i pokrenuta unutar Oracle VM Virtualbox okruženja. Ideja sustava je upravljanje i nadgledanje korisnika i računala unutar neke tvrtke te izravnu primjenu Active Directory i Group Policy nad njima.

Active Directory uvelike olakšava i pomaže u upravljanju i kontroli u većim organizacijama. Jedna od ključnih prednosti Active Directory-a je centralizirano upravljanje identitetom te upravljanje cjelokupnom mrežom unutar organizacije utemeljenoj na sustavu Microsoft Windows s jedne središnje lokacije.

Najtraženija funkcionalnost platforme Active Directory je Group Policy. Group Policy omogućava administratorima da naredbama i skriptama upravljaju većim skupinama koje koriste Windows operacijski sustav. Ključna prednost Group Policy je daljinsko upravljanje korisnicima s jedne središnje platforme.

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 Virtualbox, VMWare ili 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.

Pri učenju i shvaćanju načina na koji se može kvalitetno izraditi rad u ovom okviru, puno su pomogla znanja stečena tijekom dosadašnjeg obrazovanja. U prvom redu to se odnosi na upoznatost s Oracle VM Virtualbox aplikacije bez koje praktička realizacija ovog projekta nebi bila moguća.

6. Literatura

1. Desmond, B., i sur. (2013): Active Directory. O'Reilly Media, Inc., New York.
2. What Is Windows Server and How Is It Different From Windows?, preuzeto 2.8.2021. s https://www.makeuseof.com/tag/windows-server-different-windows/
3. How to Install Windows Server 2019 Step by Step, preuzeto 2.8.2021. s https://computingforgeeks.com/install-windows-server-2019/
4. How to Setup Active Directory Domain With VirtualBox and Join Computers, preuzeto 2.8.2021. s https://www.kindsonthegenius.com/how-to-setup-active-directory-domain-with-virtualbox-and-join-computers-part-1/
5. Microsoft Active Directory, preuzeto 2.8.2021. s https://security.foi.hr/wiki/index.php/Microsoft_Active_Directory.html
6. What is Active Directory?, preuzeto 2.8.2021. s https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx
7. Windows mreže: Koja je razlika između Workgroup i Domain?, preuzeto 2.8.2021. s https://pcchip.hr/helpdesk/windows-mreze-koja-je-razlika-izmedu-workgroup-i-domain/
8. Što je MS Active Directory?, preuzeto 3.8.2021. s https://geek.hr/pojmovnik/sto-je-ms-active-directory/
9. Understanding the Active Directory Logical Model, preuzeto 3.8.2021 s https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model
10. Network Administration: Structure of Active Directory, preuzeto 3.8.2021. s https://www.dummies.com/programming/networking/network-administration-structure-of-active-directory/
11. How to Install Active Directory Domain Services in Windows Server 2019, preuzeto 3.8.2021 s https://computingforgeeks.com/how-to-install-active-directory-domain-services-in-windows-server/
12. Guide: How to Install Active Directory in Windows Server 2019 (Server Manager), preuzeto 4.8.2021 s https://petri.com/how-to-install-active-directory-in-windows-server-2019-server-manager

13. What is Group Policy (GPO) and What Role Does It Play in Data Security, preuzeto 4.8.2021 s https://www.lepide.com/blog/what-is-group-policy-gpo-and-what-role-does-it-play-in-data-security/
14. What Are Active Directory Security Groups?, preuzeto 4.8.2021 s https://www.lepide.com/blog/what-are-active-directory-security-groups/

7. Popis slika