# Primjena sigurnosnih politika u Windows domeni

**Dolenec, Ana**

**SVEUČILIŠTE U ZAGREBU**
**FAKULTET ORGANIZACIJE I INFORMATIKE**
**V A R A Ž D I N**

**Ana Dolenec**

# Primjena sigurnosnih politika u Windows domeni

# Eng.: Security policy application in the Windows domain

**ZAVRŠNI RAD**

**Zabok, 2022.**

**SVEUČILIŠTE U ZAGREBU**
**FAKULTET ORGANIZACIJE I INFORMATIKE**
**V A R A Ž D I N**

**Ana Dolenec**
**Matični broj: 0016145989**
**Studij: Primjena informacijske tehnologije u poslovanju**

# Primjena sigurnosnih politika u Windows domeni

# Eng.: Security policy application in the Windows domain

**ZAVRŠNI RAD**

**Mentor:**

Izv. prof. dr. sc. Ivan Magdalenić

**Zabok, 2022.**

*Ana Dolenec*

**Izjava o izvornosti**

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

*Autorica potvrdila prihvaćanjem odredbi u sustavu FOI-radovi*

**Sažetak**

Ovaj rad se bavi temom na koje sve načine se mogu upotrebljavati sigurnosne politike unutar Windows domene. Postoje točno propisana pravila koje se trebaju poštivati u informacijom sustavu kako bi se postigla odgovarajuća razina sigurnosti te transparentnost. Ovdje se obrađuju razni načini kako postići spomenuto kroz praktične primjere koji su ostvareni na virtualnoj mašini unutar koje je instaliran Windows server 2019 sa kreiranom domenom. U domeni su stvorene određene grupe korisnika koje pripadaju različitim organizacijskim jedinicama u sklopu nekog informatičkog sustava koji je u ovom slučaju fiktivni. Kroz te praktične primjere dan je veliki naglasak na upotrebu Group Policy grupu sigurnosnih pravila odnosno konfiguracija postavki operacijskog sustava.

**Ključne riječi**: sigurnosna politika; Windows domena; Active Directory; Group Policy; informacijski sustav; upravljanje sigurnošću; operacijski sustav

Sadržaj

# 1. Uvod

Danas tehnologija napreduje iz dana u dan, sve više je potreba za računalnom potporom pogotovo u velikim tvrtkama sa ogromnim brojem zaposlenih. Navedeno povlači upotreba velikog broja računala koje treba na neki način održavati, administrirati kao i mrežom u kojoj se nalaze. Na sigurnost se sve više daje naglasak jer ako podaci odnosno informacije nisu sigurne, tada je cjelokupno poslovanje ugroženo i izloženo raznim rizicima. Postoje raznoliki načini kako ostvariti što bolju sigurnost informatičkog sustava uz pridržavanje određenih pravila. Svaka tvrtka bi trebala osigurati osobu ili osobe koje će biti zadužene za održavanje razine zaštite poslovnog sustava, njegovo upravljanje, nadgledanje te za unapređenje poslovne i sigurnosne politike.

U prvom poglavlju ovog rada bit će obrađena sigurnosna politika Windows domene koja se odnosi na organizaciju upravljanja sigurnošću informatičkog sustava. Uloga sigurnosne politike u poslovnom sustavu je velika i sadrži propisana pravila koje je potrebno provoditi i razvijati kako bi se izbjegli ozbiljni sigurnosni propusti ili proboji. Nadzor nad informatičkim sustavima se provodi na razne načine koje će biti objašnjeni u ovom poglavlju. Sigurnosna politika se odnosi na administratore sustava koji administriraju, vrše nadgledavanje, prate događaje na mreži. Korisnici su također dionici tog sustava koji imaju određenu odgovornost u obliku dodijeljenim im ovlasti nad određenim mrežnim resursima i ispravno rukovođenje i korištenje istih. Sigurnosna politika obuhvaća još i svu računalnu opremu koja se nalazi u sustavu. Tvrtke koje imaju vlastitu mrežu i mrežne te komunikacijske uređaje dužne su razraditi i poštivati pravila koje se odnose na njezino upravljanje. U velikom sustavu vjerojatnost pojave sigurnosnih incidenata je velika te se oni moraju detektirati i rješavati po određenim pravilima s ciljem poboljšanja funkcionalnosti samog sustava. Također ovdje će biti objašnjena i Windows domena kao i njene prednosti i nedostaci.

Drugo poglavlje je posvećeno Windows server-u 2019 i konfiguraciji domenskog sustava, što je to Windows server i koje su njegove mogućnosti. Bit će opisani tehnički koraci koje je trebalo provesti kako bi se pokazali razni načini upravljanja sigurnošću u domeni te alati kao sastavni dio servera koji se upotrebljavaju.

Treće poglavlje se odnosi na praktični dio ovog rada u kojem će biti prikazani i opisani različiti primjeri kako se u Windows domeni može administrirati te upravljati politikama sigurnosti pomoću Active Directory i Group Policy.

# 2. Sigurnosna politika Windows domene

Kada se govori o sigurnosti nekog sustava, bez obzira na njegovu veličinu, svrhu, te upotrebu, treba uzeti u obzir mnogo čimbenika, definiranih pravila koja se moraju poštivati u provođenju njegove zaštite. U nastavku će biti opisano što je potrebno poduzeti kako bi se postigla maksimalna sigurnost Windows domene.

## 2.1. Organizacija upravljanja sigurnošću

Sigurnosna politika je sastavni dio informacijskog sustava koja upravlja njegovom sigurnošću. Njezina uloga je definicija prihvatljivih i neprihvatljivih načina ponašanja, jasno raspoređivanje odgovornosti i zadataka kao i odgovarajućih sankcija u slučaju nepridržavanja navedenog. Ona se odnosi na administratore sustava, korisnike, svu računalnu opremu koja se nalazi u sustavu te po potrebi na vanjske tvrtke koje rade na održavanju opreme i programa. Svaka tvrtka koja ima vlastitu domenu trebala bi propisana pravila provoditi te eventualno prilagođavati u skladu s poslovanjem i dostupnim resursima, a sve u dopuštenim granicama koje ne ugrožavaju samu sigurnost i integritet podataka, odnosno informacija. Djelatnike je potrebno upoznati sa određenim pravilima, primjerice rukovanje date im lozinke za ulaz u domenu tvrtke, kako koristiti elektroničku poštu, korištenje baze podataka, rukovanje povjerljivim informacijama, rukovanje informatičkom opremom i to sve u skladu s vrstom posla koja im je dodijeljena. Najvažnija stvar u provođenju sigurnosne politike u informacijskom sustavu je da se u svakom trenutku točno zna što je čiji posao i tko je za što odgovoran.

Prostor u tvrtkama je obično podijeljen na dio koji je otvoren za javnost i prostor kojem imaju pristup samo zaposleni. Računala koje obavljaju funkcije neophodne za funkcioniranje informacijskog sustava i sadrže povjerljive podatke, fizički se odvajaju u prostor kojemu imaju dozvoljeni ulaz samo ovlaštene osobe, primjerice sistemska soba.

Nadzor informacijskog sustava provodi se na slijedeće načine:

- osiguranje integriteta, povjerljivosti i dostupnosti informacija
- provjera informacijskog sustava i njegovog korištenja da li je u skladu sa zahtjevima sigurnosne politike
- nadzor obavljaju osobe koje je tvrtka ovlastila
- pri provođenju nadzora ovlaštene osobe su dužne poštivati privatnost korisnika i njihovih podataka
- provođenje istrage u slučaju sumnje na sigurnosni incident

Osobe koje se u radu koriste računalima možemo podijeliti na korisnike i davatelje informacijskih usluga. Korisnici su osobe koje u svom radu koriste računala, unose podatke u bazu podataka i generiraju dokumente. Oni se moraju pridržavati određenih pravila prihvatljivog korištenja kao što je upotreba računala koja je u skladu sa važećim zakonima, etičkim normama i pravilima lokane sigurnosne politike. Navedeno se odnosi na prijavljivanje sigurnosnih incidenata u svrhu brzog rješavanja problema, odgovornost za nastale dokumente i unijete podatke te za njihovo čuvanje. Većinom u velikim tvrtkama postoje razne aplikacije za obradu poslovnih podataka i radi poboljšanja sigurnosti imenuje se jedna osoba glavnim korisnikom koji je odgovoran za provjeru ispravnosti podataka te za dodjelu dozvola za pristup podacima.

Davatelji informatičkih usluga su profesionalci koji se brinu o radu računala, mreže i cijelog informacijskog sustava. To mogu biti sistem inženjeri i članovi njihovih timova koji brinu o ispravnost i neprekidnost rada informacijskog sustava. Specijalisti za sigurnost pružaju pomoć pri rješavanju incidenata te vode brigu o sigurnosti. Oni moraju biti stručni, komunikativni i posjedovati sposobnost za vođenje ljudi.  Drugim riječima zadaća specijalista za sigurnost je ukupna briga o sigurnosti informacijskom sustava:

- fizička sigurnost – suradnja sa zaposlenicima
- nadziranje rada mreže i servisa
- organizacija obrazovanja korisnika i administratora
- komunikacija sa upravom
- sudjelovanje u donošenju odluka o nabavi računala i programa
- sudjelovanje u razvoju programa

Administratori sustava, možemo ih nazvati i domenski administratori, dodjeljuju određene ovlasti korisnicima u smislu kreiranja kvalitetne lokalne lozinke, otvaranjem organizacijskih jedinica unutar domene, dodavanjem klijentskih računala u domenu, pridruživanjem korisnika u sigurnosne grupe. Moraju administrirati računalima i mrežnom opremom u skladu s pravilima struke brinući istovremeno o funkcionalnosti i sigurnosti. Administratori sustava svakodnevno prate rad sustava, servisa i nadgledavaju rad korisnika u svrhu detekcije nedopuštenih aktivnosti. Svako računalo bi trebalo imati imenovanog administratora koji je zadužen za instalaciju i konfiguraciju potrebnih programa. Računala moraju biti konfigurirana na način da budu zaštićena od napada izvana i iznutra što se ostvaruje instaliranjem antivirusnih programa, zakrpama, listama pristupa te filtriranjem prometa. Antivirusna zaštita provodi se na nekoliko razina:

- na poslužiteljima elektroničke pošte
- na internim poslužiteljima
- na svakom računalu korisnika

Administratori brinu o lozinkama u smislu poznavanja pravila dodjele i korištenja iste. Navedeno se odnosi na minimalnu dužinu lozinke (kratku lozinku je lakše probiti), prilikom

kreiranja lozinke ne koristiti riječi iz rječnika, izmiješati velika i mala slova s brojevima te posebnim znakovima. U otvaranju nove lozinke nije preporučljivo koristiti imena bliskih osoba, ljubimaca te datume rođenja jer se takve lozinke lako otkrivaju socijalnim inženjeringom. Trajanje lozinke treba ograničiti na određeno vrijeme jer česta promjena smanjuje mogućnost njezinog otkrivanja. Korisnici su odgovorni za svoju lozinku u smislu njezinog čuvanja i ne otkrivanja. Još jedna zadaća administratora je i dodjela elektroničke adrese zaposlenicima i upoznavanje istih sa pravilima korištenja korisničkog računa i u slučaju nepridržavanja spomenutih pravila u obliku uskraćivanja prava na korištenje servisa.

### 2.1.1. Upravljanje mrežom

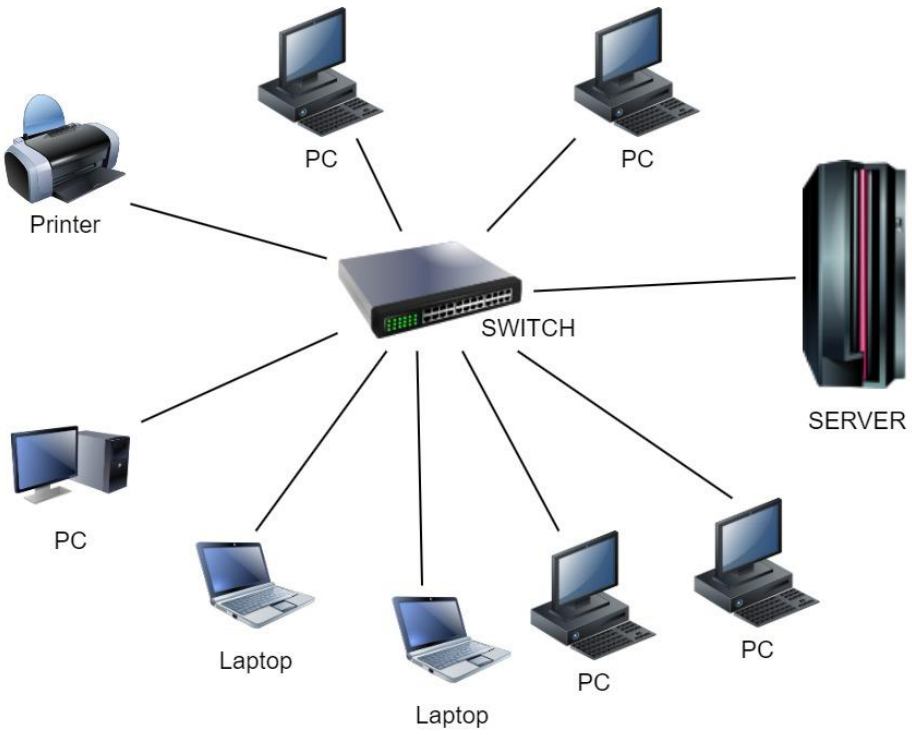
Tvrtke koje imaju vlastitu mrežu, svoje vlastite mrežne i komunikacijske uređaje moraju razraditi pravila koja određuju tko će upravljati mrežom, konfigurirati mrežne uređaje, dodjeljivati adrese te kreirati po potrebi virtualne LAN-ove. Poželjno je propisati procedure za priključivanje računala na mrežu u obliku obrazaca kojima se izdaje odobrenje za priključivanje računala na mrežu, popis svih mrežnih priključaka i umreženih uređaja. Navedeno se odnosi i na rad na daljinu gdje se djelatnici priključuju na mrežu pomoću kućnog računala ili službenog laptopa. Potrebno je osigurati da udaljeno računalo ne ugrožava sigurnost mreže od strane članova obitelji i slično. U slučaju bežične mreže potrebno je osigurati da se ne može bilo tko spojiti na privatnu mrežu i snimati promet što se ostvaruje enkripcijom i autentifikacijom uređaja i korisnika.

### 2.1.2. Sigurnosni incidenti

Kad govorimo o sigurnosnim incidentima tada se misli na njihovo upravljanje i rješavanje koje se odnosi na razrađivanju procedura. Incidente u pravilu prijavljuju zaposlenici tvrtke, koji mogu biti primjerice usporeni rad sustava, nemogućnost pristupa određenim resursima, kvar na računalu i slično. U velikoj organizaciji se u pravilu nalazi posebni dio IT podrške u obliku Service Desk-a koji zaprima, dokumentira i rješava zahtjeve koji su nastali prilikom nekog incidenta, bilo da se radi o običnom ili sigurnosnom. Administratori prate korisničke procese i u slučaju sumnje da se računalo koristi na nedozvoljen način, mogu izlistati sadržaj korisničkog direktorija, ali ne smiju provjeravati sadržaj podatkovnih datoteka. Svrha istrage incidenta je određivanje uzroka nastanka problema, sprečavanje ponavljanje istog incidenta i bolja priprema u slučaju slične situacije.

## 2.2. Windows 10 domena

Administriranje klijentskih računala može se provoditi na dva načina i to kroz Radnu grupu (eng. Workgroup) ili domenu (eng. Domain). Ovdje se obrađuje domenski način administriranja i provođenja sigurnosti sustava. Takav način je centralizirano upravljanje računalima i korisničkim računima te administrator ne treba fizički pristupiti svakom računalu nego to izvodi s jedne lokacije što u velikoj mjeri olakšava i ubrzava njihov rad. Jednostavno upravljanje korisničkim računima je jedna od prednosti ovakvog rada. Primjerice svaki korisnički račun može se koristiti na bilo kojem računalu unutar domene, korisnik može pristupati različitim resursima koji su dijeljeni, a za koje ima pravo pristupa. Navedeno mogu biti dijeljeni mrežni diskovi, mape, dokumenti, pisači i dr. Još jedna prednost ovakvog rada je upotreba Group Policy koja služi za brzu konfiguraciju i upravljanje korisničkim računima i računalima na daljinu. Na slici 1. je prikazan primjer strukture domene. Svi uređaji međusobno komuniciraju preko switch-a, a dalje se njima upravlja pomoću servera.




Slika 1: Domena (izradila autorica)

Implementacija domenske infrastrukture je skupa, zahtijeva nabavu barem jednog fizičkog servera, licenci za Windows Server te administratore koji će redovito održavati server. Za domenski rad potrebno je instalirati Windows Server na fizički ili virtualni server što će biti

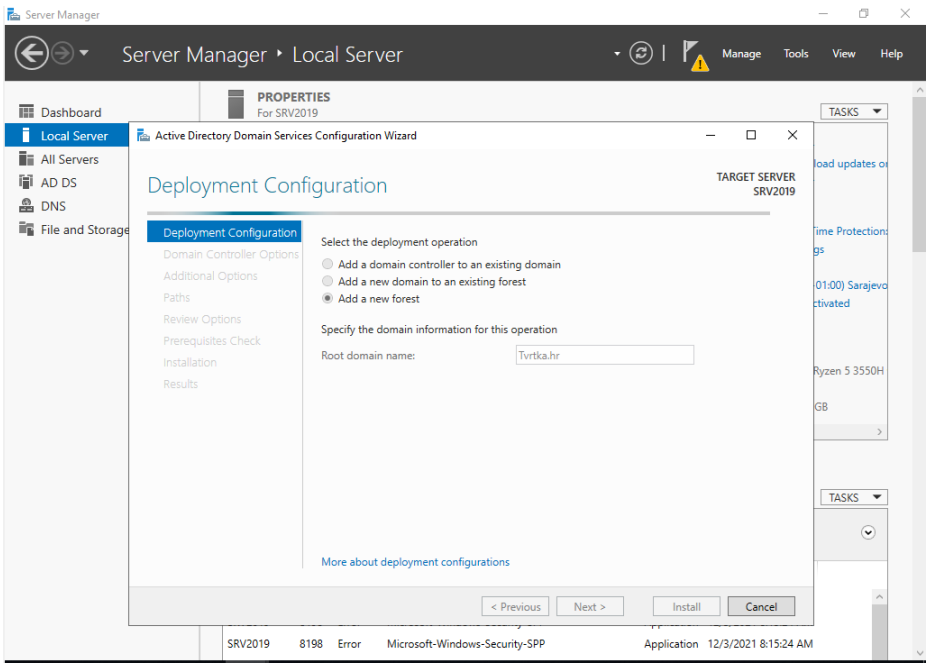
detaljnije objašnjeno u slijedećem poglavlju. Također je potrebno instalirati adekvatnu verziju Windowsa koja se može pridružiti domeni.

# 3. Windows server 2019 i konfiguracija domenskog sustava

Windows server općenito je skup operacijskih sustava koji je stvorio Microsoft za upotrebu na serveru odnosno poslužitelju. Poslužitelji su izuzetno moćne mašine koje su dizajnirane da rade non-stop i omogućavaju razne resurse za računala te se isključivo koriste u poslovne svrhe. Microsoft izdaje Windows Server pod tim imenom još od travnja 2003.g. iako je verzija servera bila i ranije dostupna pod imenom Windows NT 4.0 u radnoj verziji za opću upotrebu i za poslužitelj.

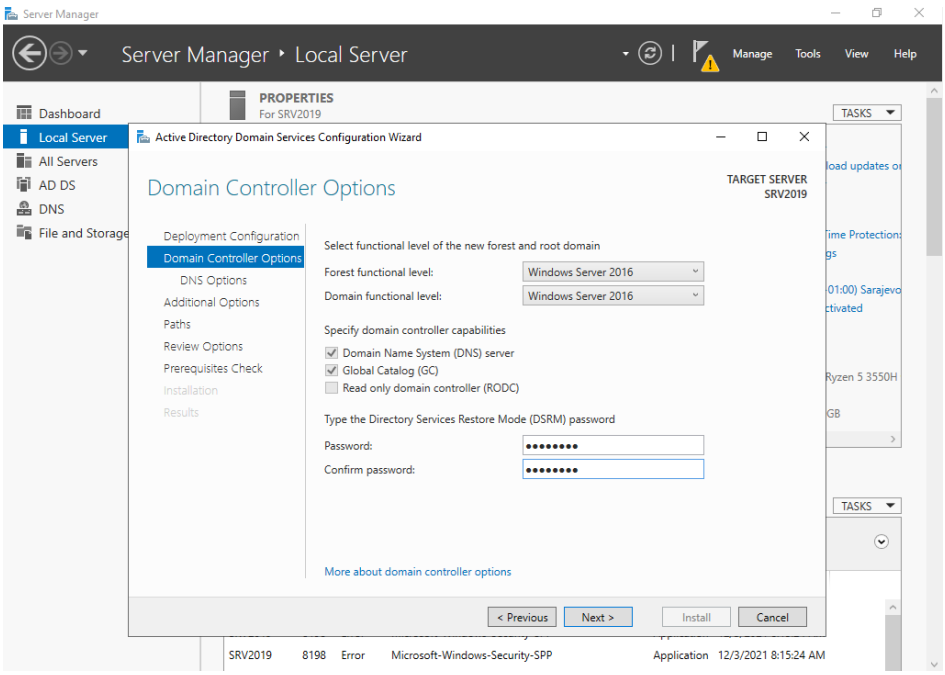
Windows Server i obični Windows (za računala) dijele puno sličnih i istih funkcija jer imaju istu bazu koda. Primjerice mogu se preuzimati i instalirati programi, radna površina izgleda isto. Svaki Windows Server lansira odgovarajuću verziju Windowsa za korisnike kao što je primjerice Windows Server 2003 verzija Windows-a XP. Verzija Windows Server 2016 je bazirana na Windows 10 Anniversary Update dok je podloga za Windows Server 2019 verzija 1809 od Windows-a 10.

Windows Server omogućava rad s mnogo poduzetnih programa koji su namijenjeni različitim svrhama. Za ovaj dio rada bilo je potrebno za početak poduzeti određene tehničke korake na računalu. Prvo sam instalirala virtualnu mašinu na računalu i unutar nje Windows Server 2019 te domensko računalo nazvala SRV2019. Slijedeći korak je konfiguracija servera u Server Manageru i dodavanje kolekciju domena (eng. *tree*) naziva Tvrtka.hr, (slika 2.).

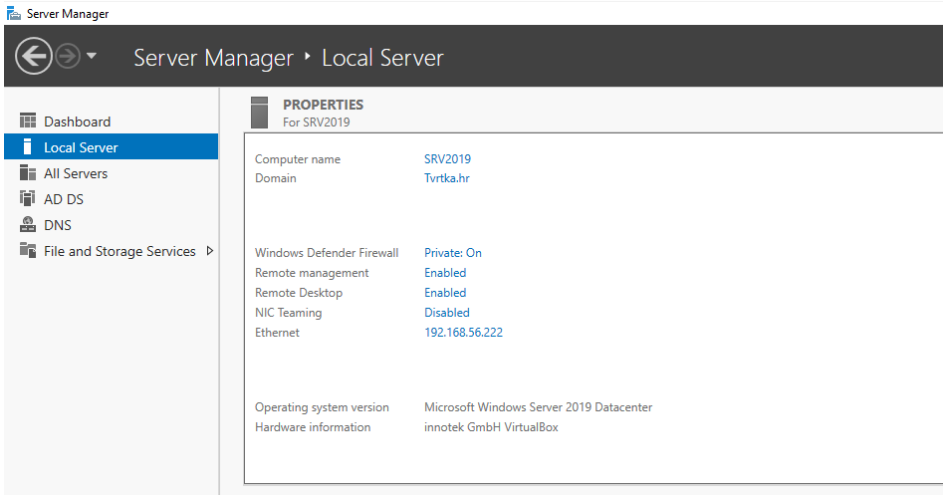



Slika 2: Kolekcija domena

U Domain Controller Options konfigurira se razina funkcionalnosti kolekcije, DNS server, globalni katalog i lozinka samog servera, (slika 3.).




Slika 3: Domain Controller Options



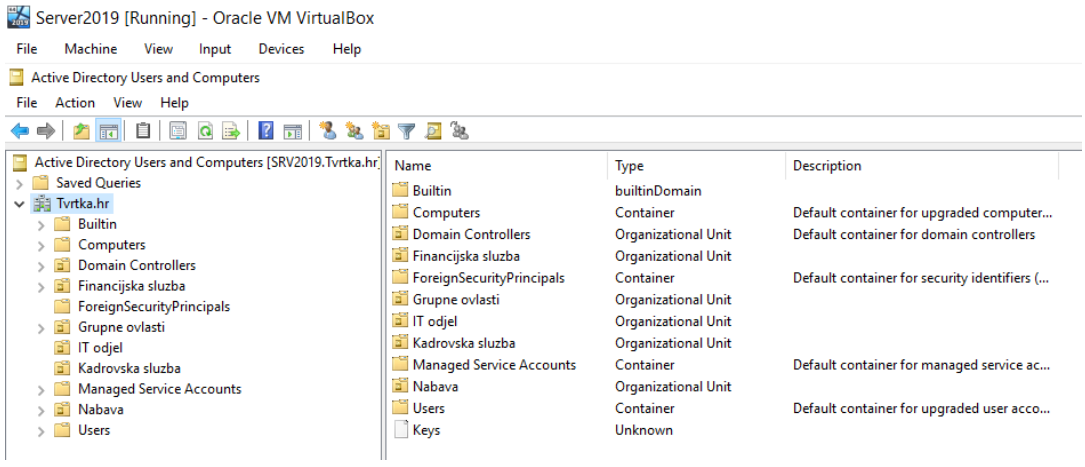

Slika 4: Local Server

Na slici 4. su prikazani detalji lokalnog servera nakon završene konfiguracije sa nazivom poslužiteljskog računala SRV2019, domenom Tvrtka.hr, te IP adresom 192.168.56.222.

## 3.1. Active Directory

Active Directory (u daljnjem tekstu AD) je upravljački servis koji omogućava administratorima da upravljaju domenom, korisničkim računima, klijentskim računalima, sustavom, uređajima, programima, pohranom podataka, mrežom, SaaS servisima i mnogim drugim resursima. AD također omogućava serveru da se ponaša kao domain controller što znači da obrađuje zahtjeve od autentičnih korisnika unutar domene, te upravlja dozvolama i pristupom na mrežne resurse. On sprema podatke kao objekte koji mogu biti korisnici, grupe, programi ili uređaji.

Glavni servis u AD-u je Domain Services (AD DS) koji sprema informacije i upravlja interakcijom korisnika sa domenom. Verificira pristup korisnicima na server i mrežu te kontrolira za svakog korisnika kakvu ovlast ima za pristupanjem mrežnim resursima. Active Directory Domain Services koristi slojevitu strukturu koja se sastoji od domena, grupa domena i kolekcije grupa domena. U njemu svaki server i radna stanica moraju biti član samo jedne domene i locirani samo na jednoj stranici, (eng. *site*). Na slici 5. je prikazana struktura domene koja je kreirana za potrebe ovog rada. Domena naziva Tvrtka.hr sastoji se od grupe objekata kao što su korisnici, uređaji i organizacijske jedinice koji moraju biti jedinstveni. Jedinstvenost se odnosi na primjer na korisničke račune koji ne smiju imati ista korisnička imena. Kreirane su i neke grupne ovlasti odnosno sigurnosne grupe naziva Financije R i Financije RW koje će biti objašnjenje u praktičnom dijelu ovog rada.




Slika 5: Struktura u Active Directory Users and Computers

AD ima i još neke servise:

- Lightweight Directory Services (AD LDS) – slične funkcionalnosti kao i AD DS. Može biti pokrenut u višestruke instance na jednom serveru i čuva podatke u spremištu koristeći servis Lightewight Directory Access Protocol.

- Lightweight Directory Access Protocol (LDAP) – aplikacijski protokol koji se koristi za pristup i održavanje servisa nad mrežom.
- Certificate Services – generira, upravlja i dijeli certifikate. Certifikat koristi enkripciju sa javnim ključem kako bi omogućio razmjenu podataka preko interneta.
- Active Directory Federation Services – autentificira korisnike na više programa koristeći single sign-on (SSO). SSO je servis koji dopušta korisniku da koristi jedan set vjerodajnica za prijavu.
- Rights Management Services – kontrolira prava informacija i upravlja njima. On šifrira sadržaj primjerice u Word dokumentima koji se šalju putem elektroničke pošte na serveru.

## 3.3. Group Policy

Group Policy, (u daljnjem tekstu GP), je centralizirana konfiguracija postavki i upravljanja operacijskim sustavom, postavkama računala i korisnika u Microsoft IT okolini, odnosno domeni. Drugim riječima GP je domenska funkcionalnost koja omogućava uređivanje postavki lokalnog klijenta sa središnje lokacije na serveru. Priključivanje računala Active Directory domeni samo po sebi nema nekih posebnih prednosti ako ne koristimo jednu od domenskih prednosti kao što je GP ili pravilnici skupine koji se sastoje od korisničkih i računalnih postavki koje se mogu primijeniti za vrijeme pokretanja računala ili prijave korisnika u sustav. Navedene postavke se mogu primjenjivati za prilagođavanje korisnikove okoline, sigurnosnih okvira, omogućavanje što jednostavnije korisničke i računalne administracije. Na svakom računalu postoji početno jedan lokalni pravilnik čije se postavke prepisuju postavkama iz Active Directory pravilnika skupine.

Group Policy Object, (u daljnjem tekstu GPO), je politika odnosno skup pravila kojima se korisnicima u domeni podešavaju i mijenjaju postavke na način da se na njih primjeni skup tih stvorenih pravila. GPO se sastoji do dva dijela:

- Group Policy Container (GPC) – objekt Active Directory-a koji sprema verziju informacija, njihov status i ostale informacije.
- Group Policy Template (GPT) – koristi se za spremanje podataka u obliku datoteka, programa same politike, skripte te raspoređivanje određenih informacija.

### 3.3.1. Group Policy u ulozi sprečavanja sigurnosnih ispada

GP postavke možemo konfigurirati na različite načine i u različite svrhe. Jedan od najvažnijih primjena GP-a je stvaranje sigurnosnih pravila kako bi se spriječio neovlašteni pristup sustavu, neovlašteno korištenje lozinku, povlaštenih i tajnih informacija i slično. Među važnijim sigurnosnim postavkama GP-a možemo svrstati slijedeće:

- upravljanje pristupu upravljačke ploče na računalu
- kontrola pristupa naredbenom retku, eng. *Command Promt*
- omogućavanje vanjskih jedinica kao što su DVD, CD, USB drive
- zabrana instalacija pojedinih programa na računalo
- onemogućen pristup određenim mrežnim resursima
- kreiranje i uređivanje dijeljenih mrežnih mapa i diskova u smislu dodjele prava pristupa
- onemogućavanje pristupa određenim korisnicima na računalo i dio resursa na njemu
- postavljanje minimalne i maksimalne duljine lozinke za pristup sustavu

U praktičnom dijelu ovog rada bit će opisane neke od gore navedenih postavka.

### 3.3.2. Group Policy Management Console (GPMC)

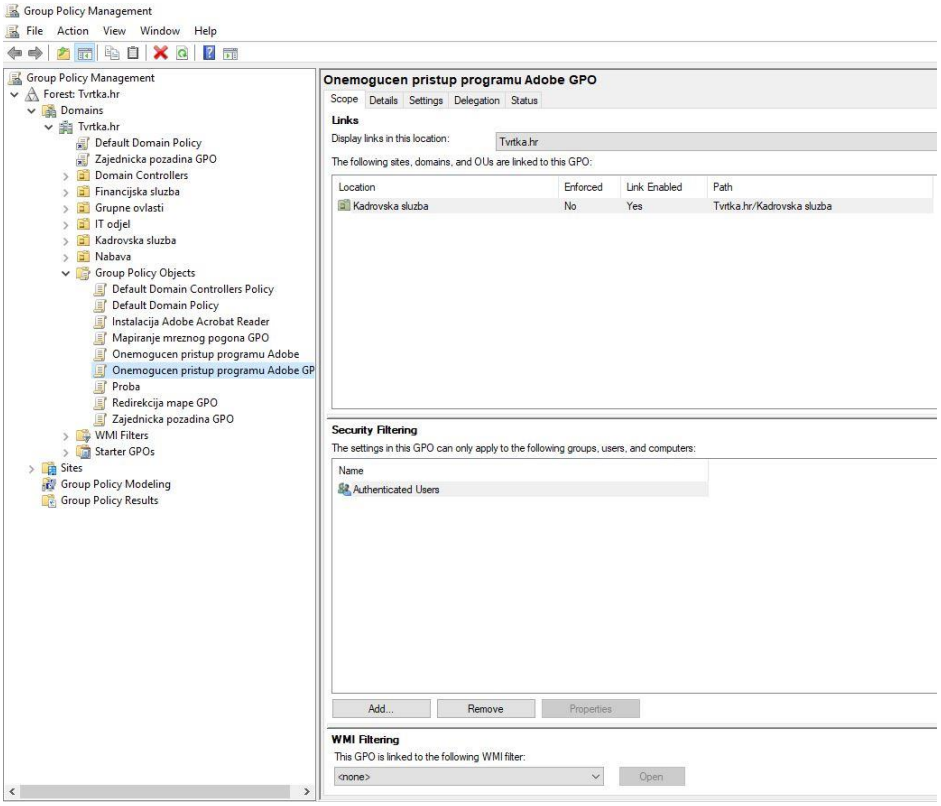
Group Policy Management Console, (u daljnjem tekstu GPMC) ili konzola za upravljanje Group Policy je dio Windows Servera operacijskog sustava još od verzije Windows Server 2008. U prijašnjim verzijama servera nije bila njihov sastavni dio. GPMC je kreirana za administratore sustava kako bi im omogućila kolekciju funkcija koje mogu primjenjivati nad domenom i sustavom, (slika 6.). Alati koje konzola ima su:

- Active Directory Users and Computers
- Active Directory Sites and Services
- Rasultant Set of Policy
- ACL Editor
- GPMC Delegation Wizard

Konzola pruža puno funkcionalnosti u gore navedenim alatima, a neke od njih su:

- korisničko sučelje koje olakšava upotrebu i upravljanje GPO-om
- backup, vraćanje podataka iz arhive

- pristup programima za provođenje GPO-a
- kreiranje, brisanje, mijenjanje GPO-a
- linkanje GPO-a
- pretraživanje GPO-a
- izvještavanje postavka GPO-a




Slika 6: Group Policy Management Console

# 4. Praktični dio – primjena sigurnosnih pravila u Windows domeni

Praktični dio će biti prikazan kroz niz primjera kako primjeniti Group Policy na većem broju računala i korisnika u nekoj tvrtci. Group Policy i primjena njezinih politika na računalima uvelike olakšava administratorima da postave neka pravila, sigurnosna rješenja, te njihovo praćenje.

U ovom radu je kreirana neka tvrtka sa računalima i korisnicima. Potrebno je bilo za početak poduzeti određene tehničke korake na računalu. Prvo sam instalirala virtualnu mašinu i unutar nje Windows Server 2019 i računalo Windows 10, te podesila postavke DNS servera. U Active Directory Users and Computer kreirala sam kolekciju domena (eng. *tree*). U ovom slučaju je jedna domena naziva Tvrtka.hr, a unutar nje sam otvorila mape računala (eng. *Computers*), korisnici (eng. *Users*), te mape odjela (Financijska služba, IT odjel, Kadrovska služba, Nabava). Unutar odjela su korisnici za koje su definirana neka osnovna pravila. U nastavku ću prikazati neke od mnogih mogućnosti Group Policy i upravljanja sigurnošću u svojstvu sigurnosnih pravila unutar Windows domene.

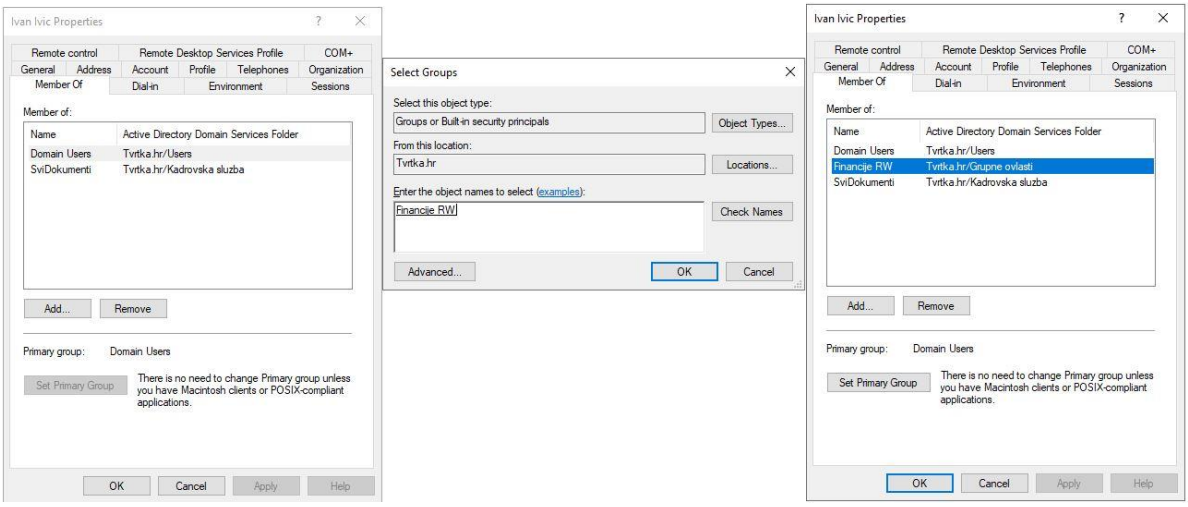
## 4.1. Grupe korisnika i prava pristupa

Grupe korisnika se koriste kako bi se na jednom mjestu moglo upravljati sa više korisničkih računa u domeni. Navedeno olakšava upravljanje mrežnom sigurnošću i omogućuje brže administriranje korisnika. U ovom primjeru ću pokazati različite grupe korisnika, te njihova prava pristupa na različite resurse unutar domene.

U prvom primjeru sam kreirala dvije grupe u mapi Grupne ovlasti kako bi mogla u njih dodala određene korisnike koji trebaju imati određena prava pristupa. Grupe sam nazvala Financije R i Financije RW. Recimo da se u odjelu Financijska služba na određenom dijelu mrežnog diska servera nalaze mape u kojima su dokumenti potrebni za rad. Grupa Financije R ima pravo samo čitanja i pregledavanja dokumenata, dok korisnici u grupi Financije RW mogu čitati, pregledavati, mijenjati, dodavati, te brisati dokumente. Nekim korisnicima je potrebno dodijeliti pravo da mogu samo čitati dokumente, a nekima da mogu dodavati nove, te postojeće mijenjati. U odjelu Kadrovska služba su dva korisnika Ivan Ivic i Marko Peric. Marku je potrebno dodijeliti pravo da može samo čitati, pregledavati navedene dokumente, dok Ivanu treba dodijeliti osim za čitanje i pravo za mijenjanje istih. Navedeno se može provesti u Active Directory na dva

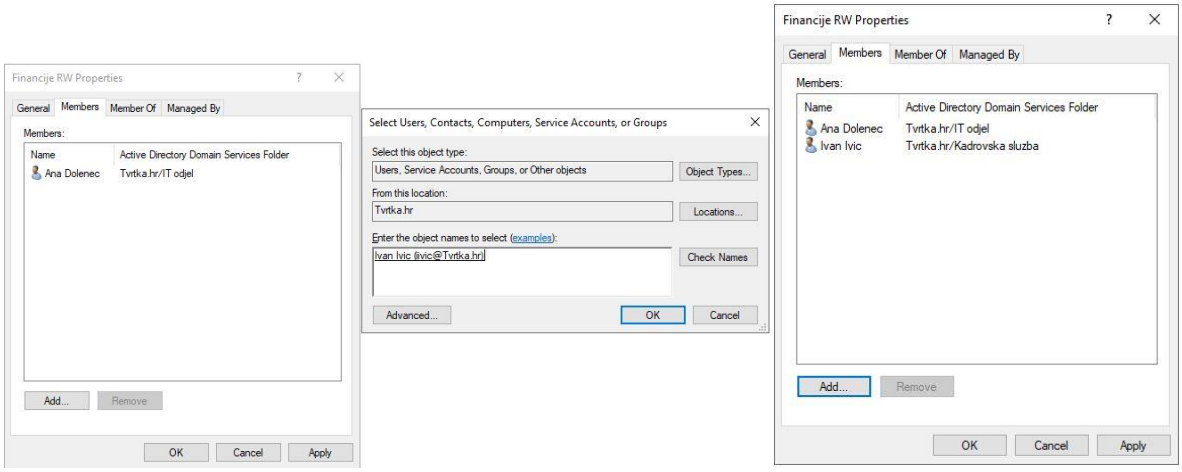
načina i to: preko korisnika da mu se doda određena grupa i preko same grupe na način da se korisnik doda u nju. Prikazano će biti oba načina.

1. Korisniku se dodaje određena grupa. Korisnik Ivan Ivic je u odjelu Kadrovska sluzba i odlaskom na detalje otvaramo karticu Member Of. Na opciji Add otvara se slijedeći ekran u kojem je potrebno upisati naziv grupe u koju ga želimo dodati. Provjerom imena grupe potvrđujemo točan odabir, te primjenom dodajemo korisniku traženu grupu (slika 7.).



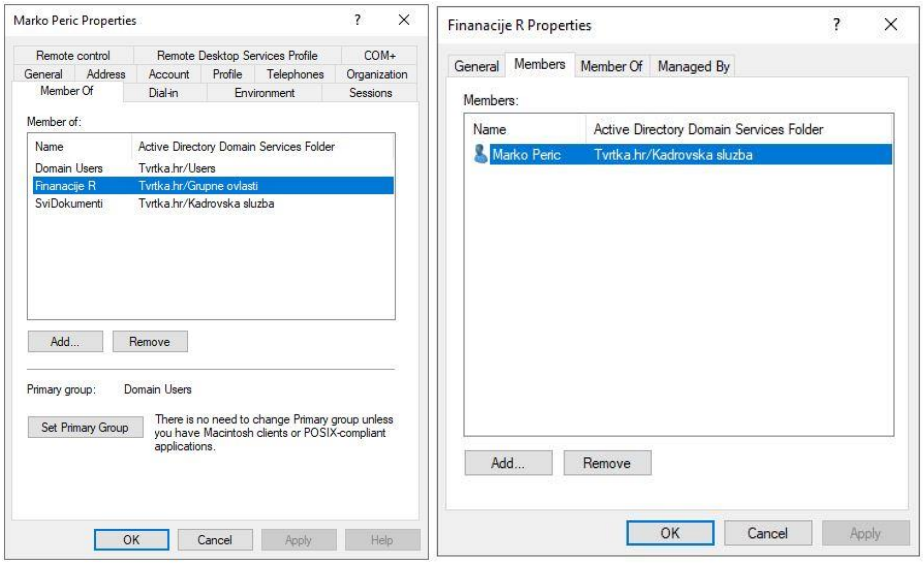

Slika 7: Dodavanje grupe korisniku

2. U grupu se dodaje određeni korisnik. U mapu Grupne ovlasti odabire se grupa Financije RW i na kartici Members dodaje se korisnik. Opcijom Add otvara se novi prozor i upisuje se ime korisnika kojeg je potrebno dodati. Nakon provjere imena potvrđujemo odabir i korisnik je dodan u grupu (slika 8.).




Slika 8: Dodavanje korisnika u grupu

Na iste načine je dodano pravo i za korisnika Marka u grupu Financije R (slika 9.).

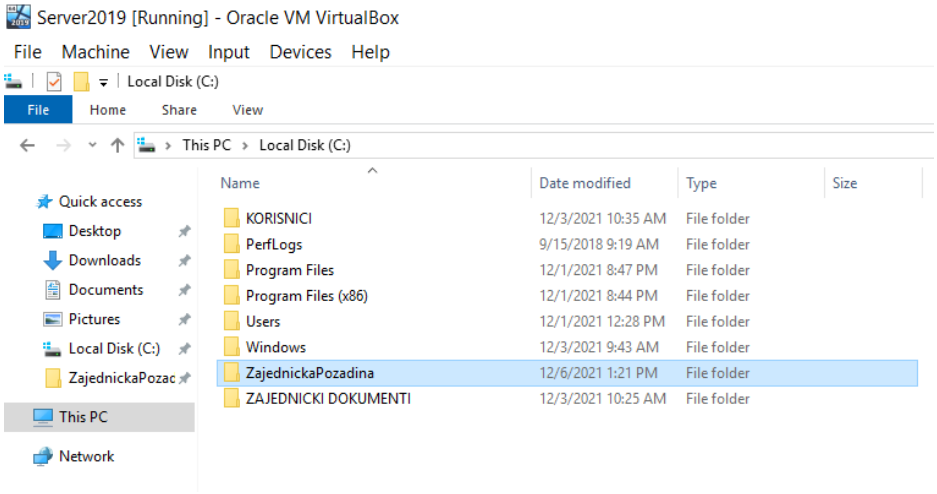



Slika 9: Dodan korisnik u grupu Financije R

## 4.2. Promjena slike pozadine na računalima

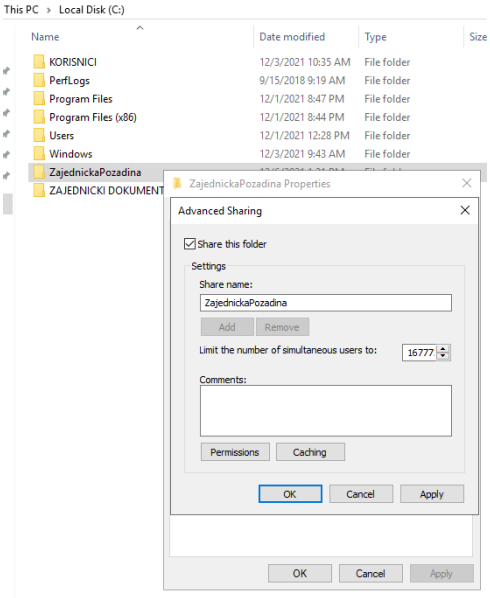
U ovom primjeru će biti detaljno prikazano kako konfigurirati promjenu pozadinske slike za klijentsko računalo. Tu ćemo primijeniti pravilo Group Policy za određenog korisnika u domeni, a može se to isto definirati za sve klijente u domeni, odnosno po potrebi poslovanja, pravila itd.

Za početak moramo imati pripremljenu sliku koju je potrebno kopirati u mapu na lokalnom disku servera koju smo nazvali ZajednickaPozadina, (slika 10.).

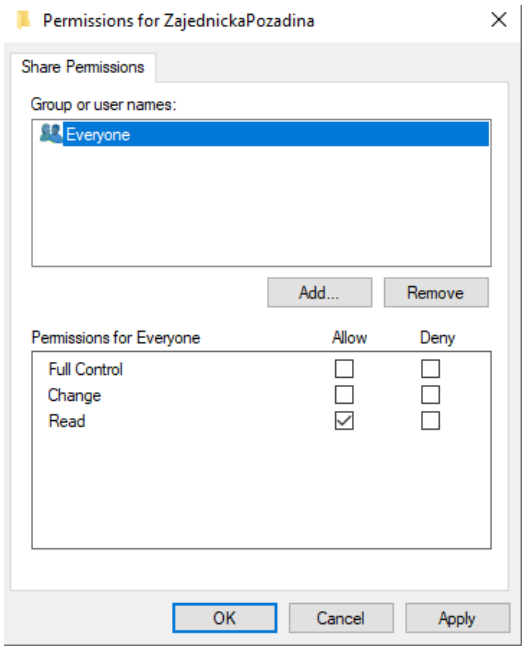



Slika 10: Mapa na disku servera

Navedenu mapu potrebno je podijeliti sa određenim klijentima u domeni i odrediti određena ovlaštenja. U ovom primjeru je dodana ovlast za sve korisnike, (slika 11. i 12.).

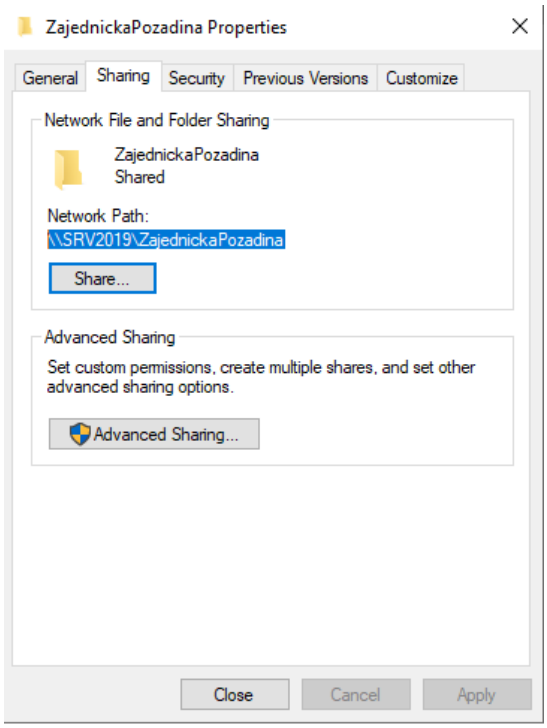



Slika 11: Dijeljenje mape



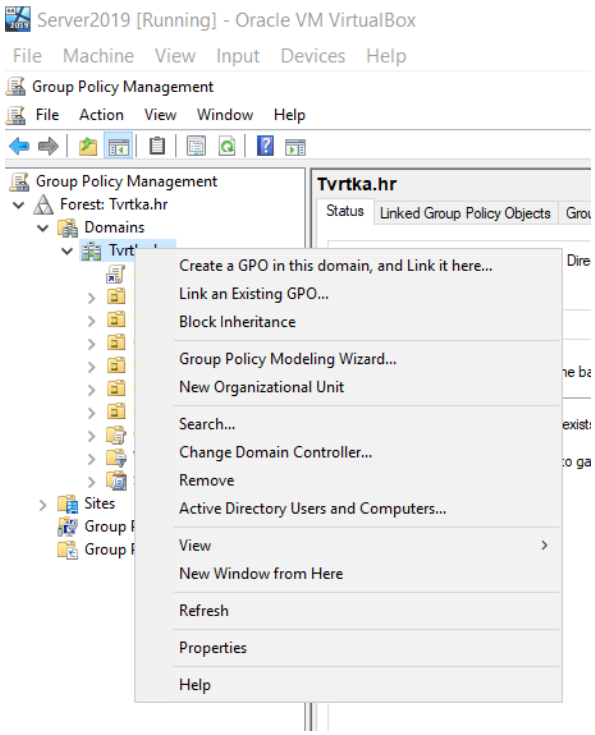

Slika 12: Određivanje ovlasti za mapu

Nakon toga je potrebno još kopirati Network Path - putanja dijeljene mape, koja će nam biti potrebna u daljnjim koracima u provođenju pravila, u našem slučaju je to: \\SRV2019\ZajednickaPozadina, (slika 13.).



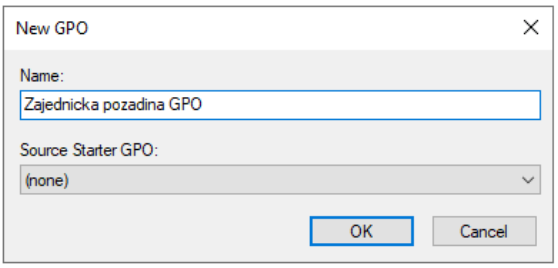

Slika 13: Network Path

Nakon definicije pravila dijeljenja i dozvola, sljedeći korak je otvoriti Server Manager Group Policy Management i na nivou domene Tvrtka.hr kreirati Group Policy Object, (slika 14.).



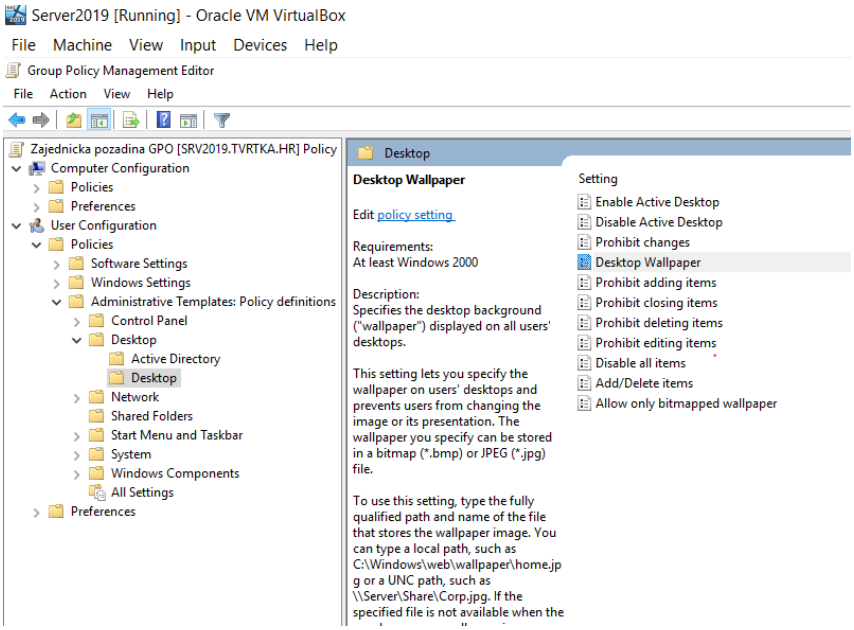

Slika 14: Kreiranje GPO na razini domene

Potrebno je odrediti naziv GPO-a, (slika 15.).



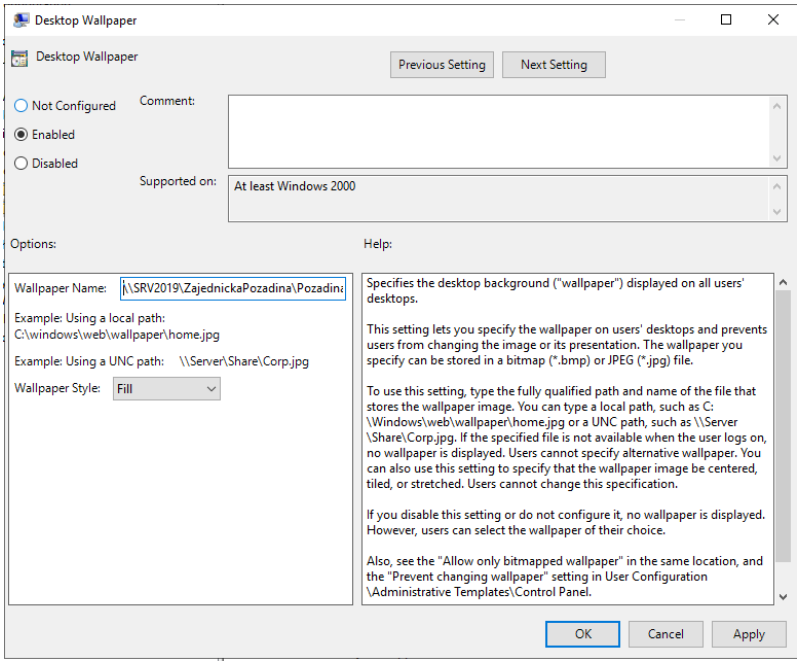

Slika 15: Naziv GPO-a

Sljedeći korak je editiranje odnosno uređivanje GPO-a koju smo kreirali pod nazivom Zajednicka pozadina GPO te pod User Configuration ići na Policies\Administrative Templates: Policy definitions\Desktop\Desktop i u desnom ekranu odabrati Desktop Wallpaper, (slika 16.).




Slika 16: Desktop

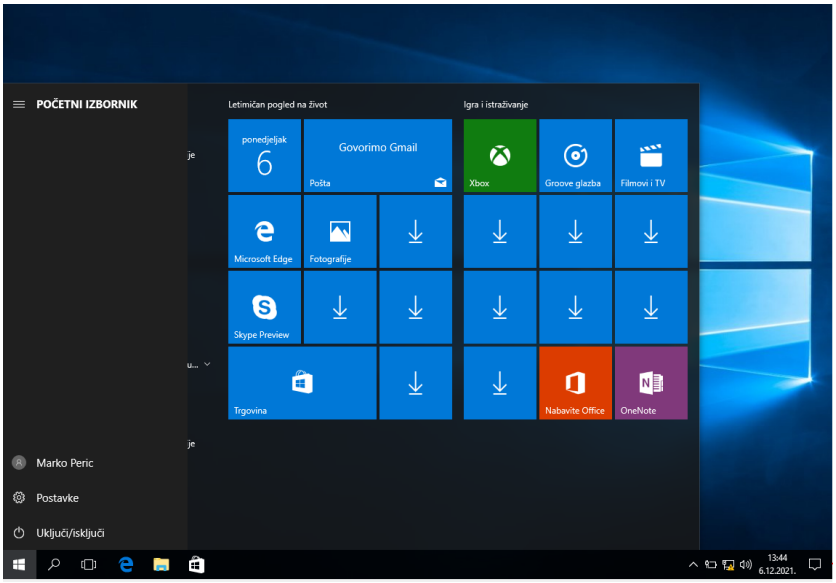
Odabirom Desktop Wallpaper otvara nam se ekran u kojem je potrebno omogućiti pravilo (Enable) i unijeti točnu putanju gdje se nalazi slika pozadine. Tu upisujemo onu putanju koju smo kopirali ranije (\\SRV2019\ZajednickaPozadina\Pozadina.png), (slika 17.).



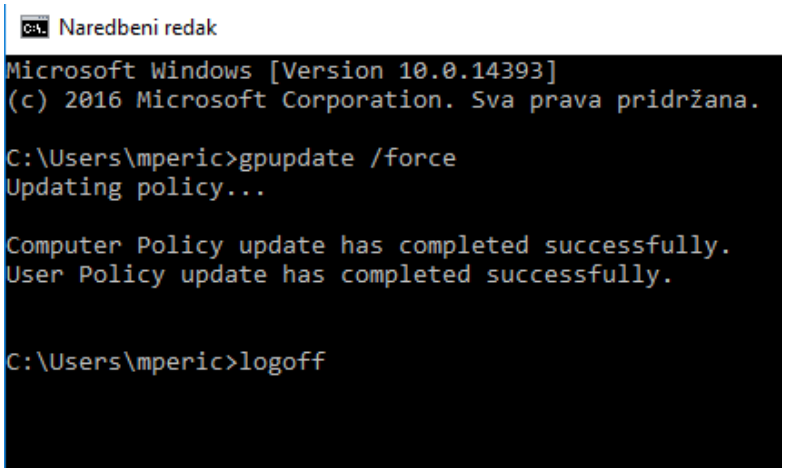

Slika 17: Desktop Wallpaper

Nakon toga se u virtualnoj mašini prebacuje na klijentsko računalo, (slika 18.). U Command Promptu (naredbeni redak) „forsa“ se (pokreće se) Group Policy putem naredbe gpupdate /force i nakon toga slijedi odjava korisnika iz računala pomoću naredbe logoff i ponovna prijava, (slika

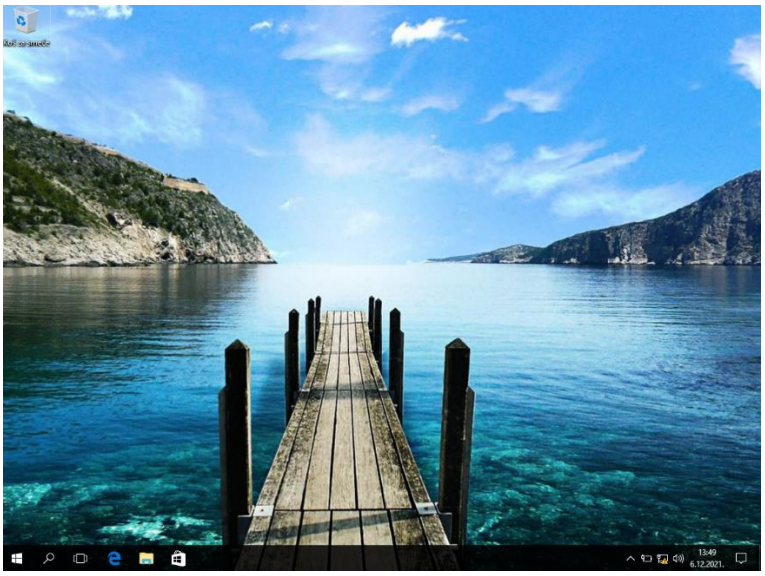
19.). Nakon ponovne prijave vidimo da se pozadinska slika promijenila i da korisnik nema mogućnosti nakon toga sam promijeniti tu sliku, (slike 20. i 21.).



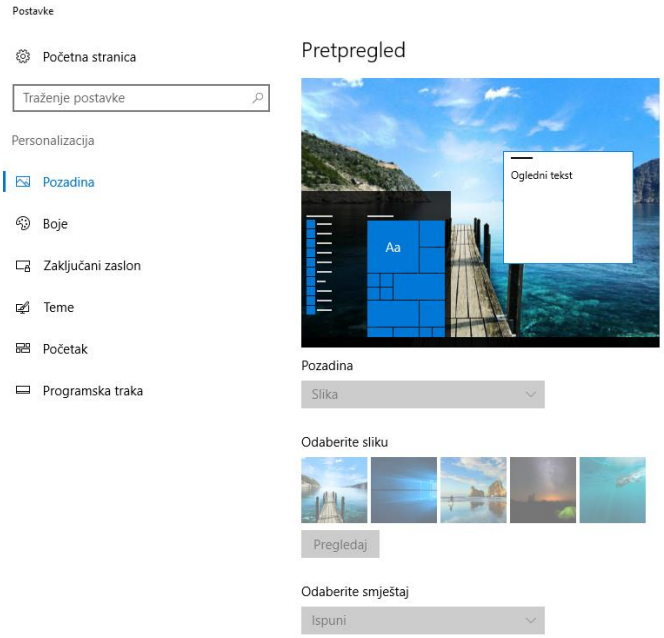

Slika 18: Klijentsko računalo




Slika 19: Command Prompt (naredbeni redak)



Slika 20: Nova slika pozadine

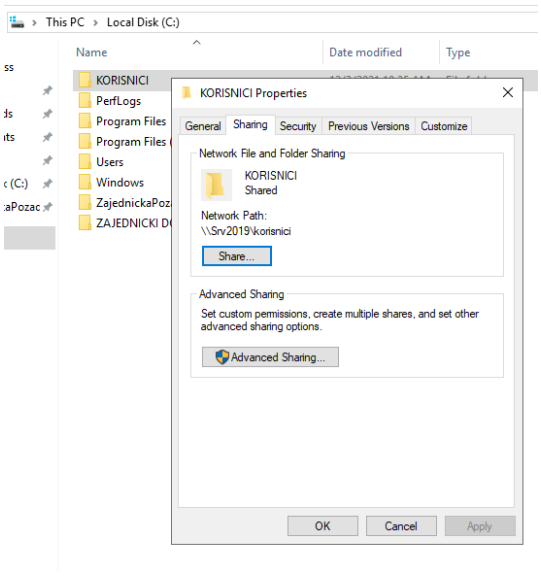



Slika 21: Nemogućnost promjene slike pozadine kao korisnik

## 4.3. Mapiranje mrežne mape pomoću skripte prilikom prijavljivanja korisnika na računalo

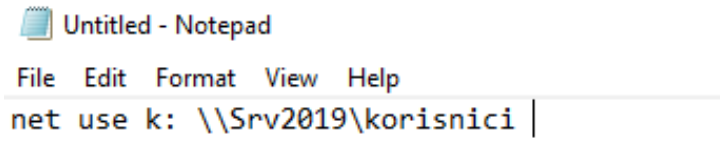
Na mrežnom disku servera kreirala sam mapu naziva korisnici u koju djelatnici tvrtke spremaju svoje dokumente. Cilj ovog primjera je da se ta mapa poveže sa svim korisnicima u domeni kako bi isti mogli pospremati i pristupiti svojim dokumentima i da se svi važni dokumenti nalaze u istoj mapi na mreži.

Prvi korak je da mapu koja se želi mapirati, proglasi dijeljenom mapom. U našem primjeru mapa se zove korisnici i nalazi se na mrežnom disku na serveru.U detaljima je vidljivo da je navedena mapa dijeljena sa svim korisnicima. Putanja se kopira jer će trebati u jednom od sljedećih koraka, (slika 22.).



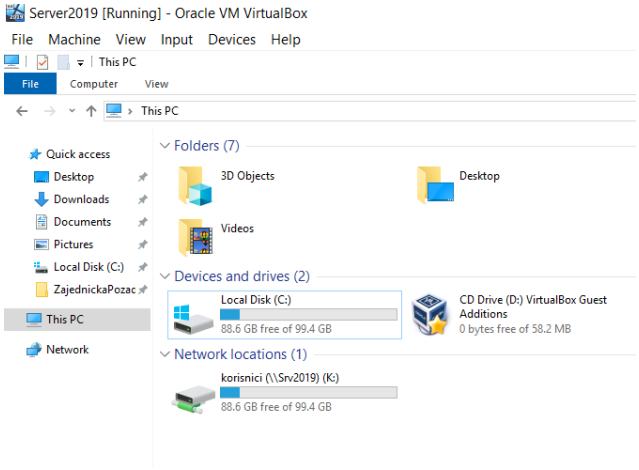

Slika 22: Dijeljena mapa

Slijedeće je potrebno kreirati bat datoteku odnosno skriptu koja će mapirati mapu kao mrežni disk. U tekstualnom editoru se upisuje naredbu net use, proizvoljno određujemo slovo na koje će se mapirati. U ovom slučaju odabrano je slovo k i ubačena putanja mape koja je prije kopirana, (slika 23.).



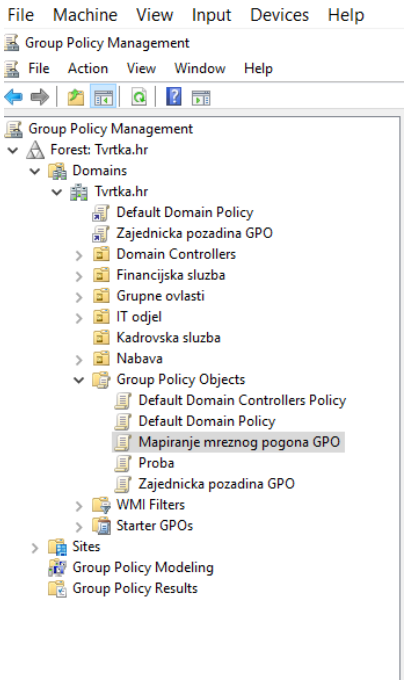

Slika 23: Bat datoteka

Datoteka je spremljena na radnu površinu servera pod nazivom *map.bat*. Sada treba prvo provjeriti da li je skripta ispravna tako da se pokreće na računalu servera i provjerava da li se mrežni pogon mapirao na server. Na slici je vidljivo da je skripta ispravna i da smo uspjeli mapirati mapu, (slika 24).



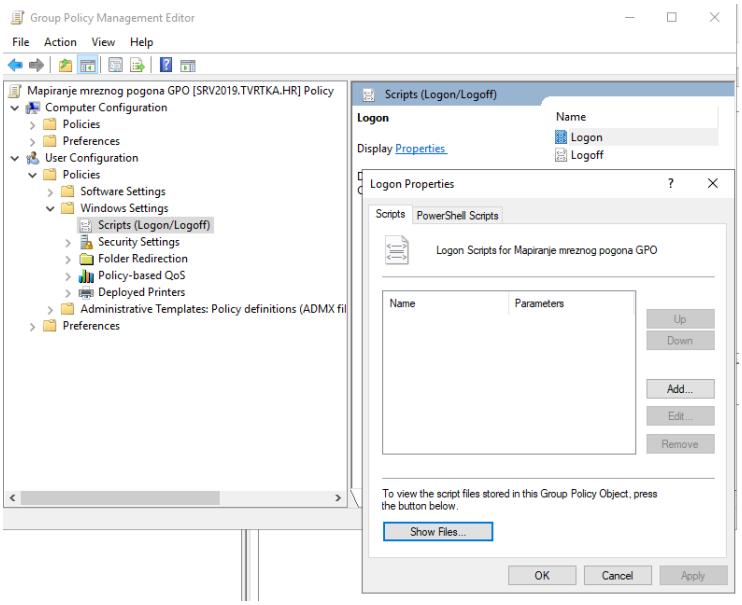

Slika 24: Mapirana mapa

Sada kada je provjerena ispravnost skripte, prebacuje se u Group Policy Management konzolu i slijedi konfiguracija GPO-a. U Group Policy Management kreirana je GPO pod nazivom Mapiranje mreznog pogona GPO, (slika 25.).



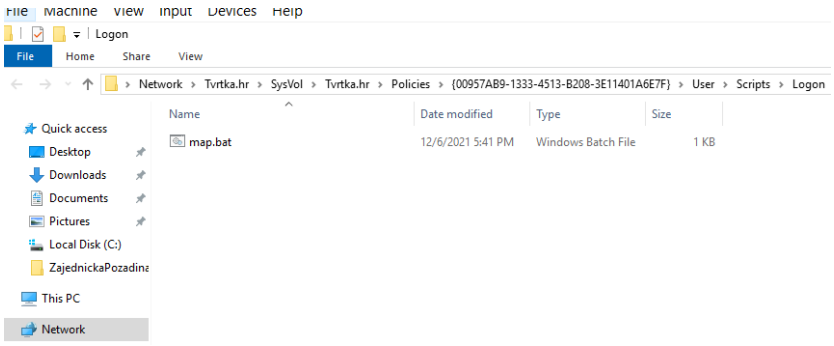

Slika 25: Kreirana GPO

Prelazimo na uređivanje GPO-a. Potrebno je odabrati opciju Logon jer radimo policy za mapiranje prilikom prijavljivanja korisnika na mrežu, (slika 26.).



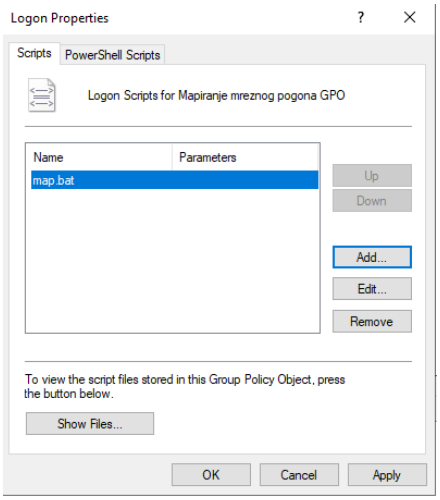

Slika 26: Logon opcija

Pod opciju Show Files otvara se konzola koja je lokacija na kojoj je naša policy i u koju moramo kopirati našu skriptu, (slika 27.).



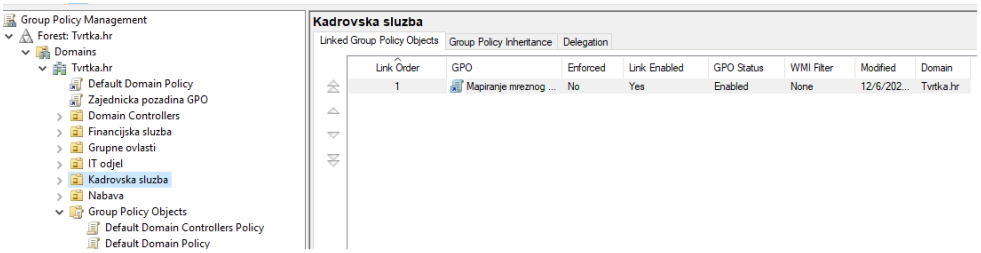

Slika 27: Konzola GPO

Potrebno je još i dodati skriptu u GPO, (slika 28.).

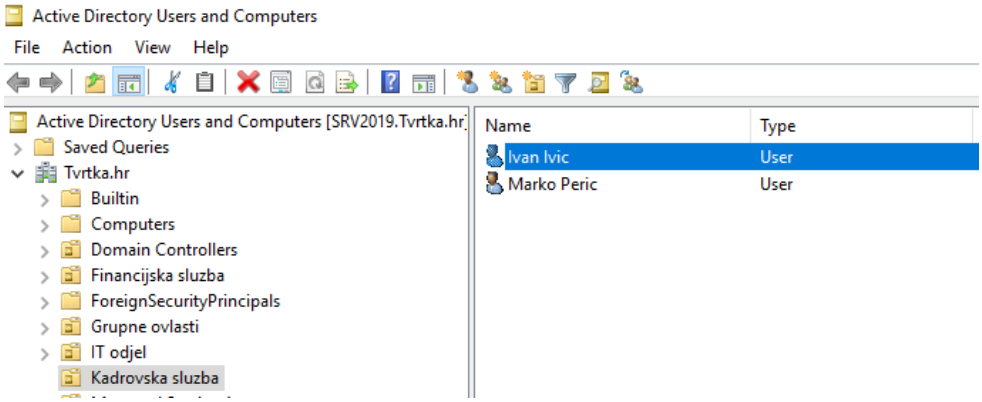



Slika 28: Dodavanje skripte u GPO

Sada ćemo povezati GPO sa odjelom naziva *Kadrovska*, (slika 29.), u kojem su dva korisnika (slika 30.).

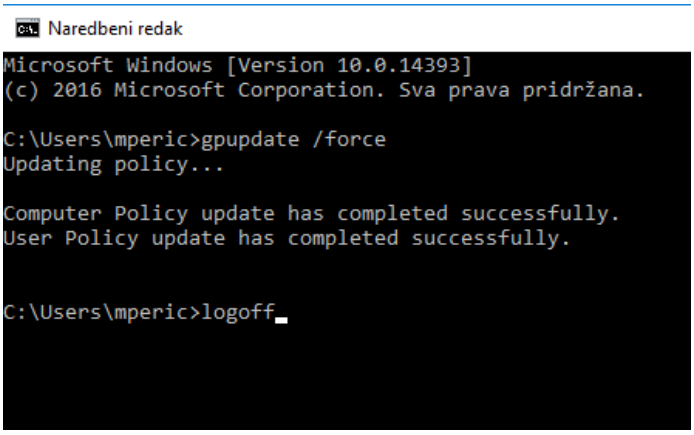



Slika 29: Povezivanje GPO

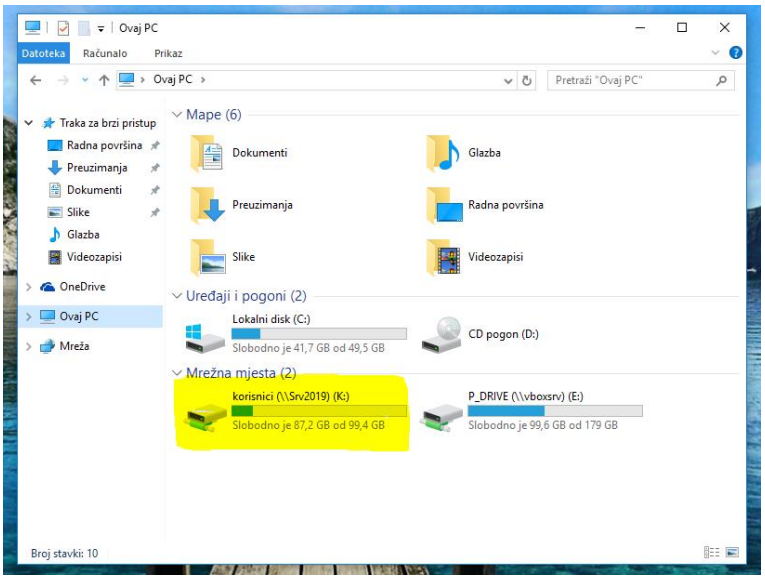



Slika 30: Korisnici u Active Directory

Prijavit ćemo se na klijentsko računalo kao korisnik Marko Peric i preko Command Prompta pokrenuti gpupdate / force kao i u prošlom primjeru, te odjaviti korisnika sa računala, (slika 31.) i ponovo prijaviti kako bi se promjena izvršila odnosno kako bi se mapirao mrežni pogon, (slika 31.). Na slici 32. je vidljivo da se primjena GPO-a uspješno provela.




Slika 31: Command Prompt

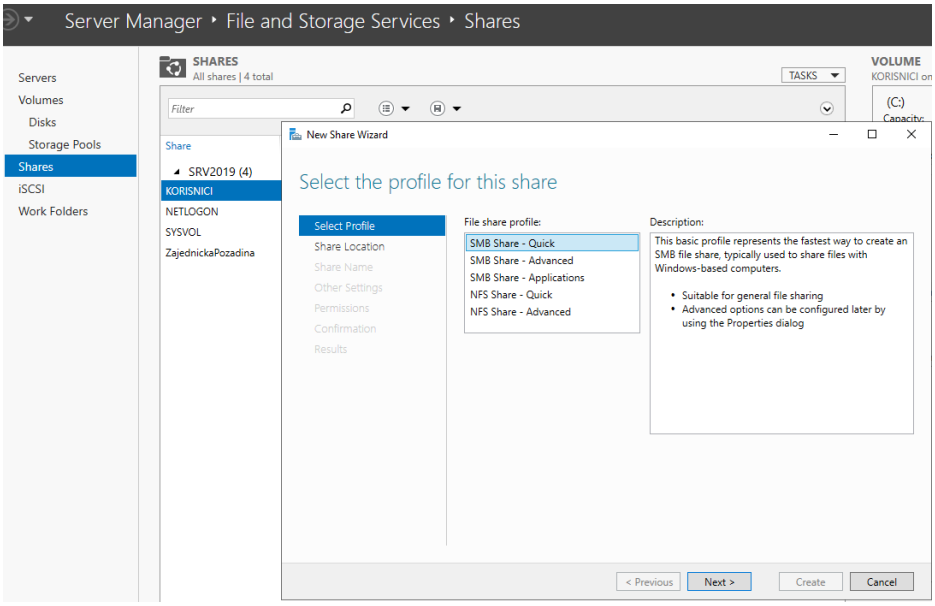



Slika 32: Mapirani mrežni pogon K

## 4.4. Preusmjeravanje mapa

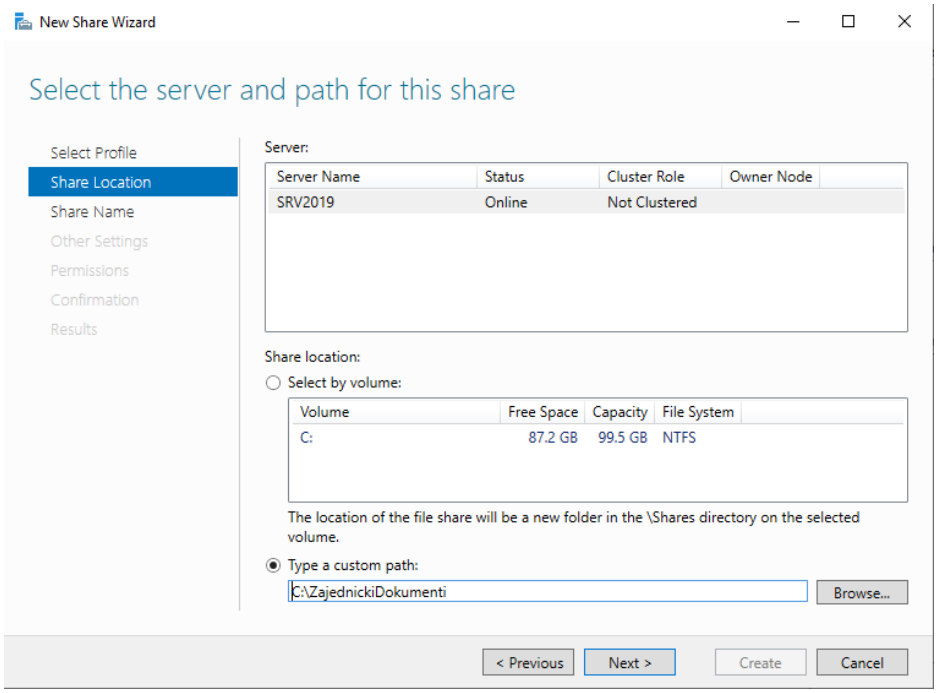
Recimo da u nekoj firmi nadređeni želi da svi zaposlenici spremaju dokumente u određenu mapu na nekoj lokaciji na serveru. Zadana lokacija za spremanje dokumenata na računalu za pojedinog korisnika je C:Users\mperic\Documents. Pomoću GPO-a ćemo definirati da sve dokumente koje korisnik sprema naočigled u mapu Documents automatski će se pohranjivati u određenu mapu na nekoj lokaciji na serveru. Korisnik će odabirom na svoju lokaciju Documents pristupati udaljenoj mrežnoj lokaciji, a ne lokalnoj mapi pritom ne primjećivati razliku. To je zapravo vrlo korisna opcija u velikim firmama sa puno zaposlenika od kojih se velika većina ne snalazi u mapama i podmapa pa spremaju dokumente lokalno. Vrlo često se zna dogoditi da te dokumente nehotično obrišu, a kasnije ih trebaju. Zato ovaj način preusmjeravanja dokumentana na mrežnu lokaciju je dobar jer i u slučaju da ga korisnik i tamo obriše, dokument se može vratiti nazad pomoću backup-a koji se pušta u pravilu svaki dan za mrežne pogone na serveru. Još jedna prednost ovakvih postavka je da korisnik može na taj način pospremati dokumente s bilo kojeg računala na kojem se prijavi jer ćemo definirati GPO kroz konfiguraciju korisnika.

Prvo moramo kreirati dijeljenje u Server Manageru pod File and Storage Services\Shares\New Task, (slika 33.).



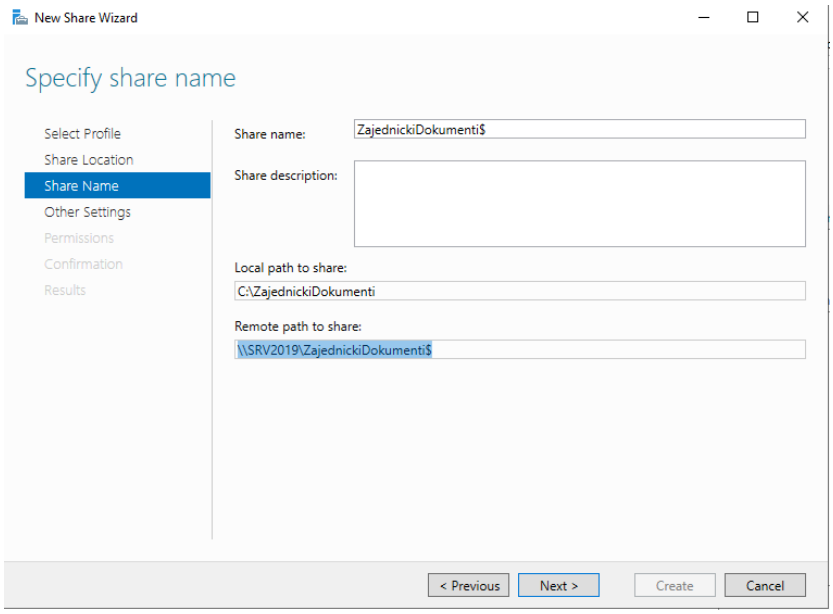

Slika 33: New Tasks

Sljedeći korak je odabrati putanju do određenog foldera, u našem slučaju je to C:\ZajednickiDokumenti, (slika 34.).



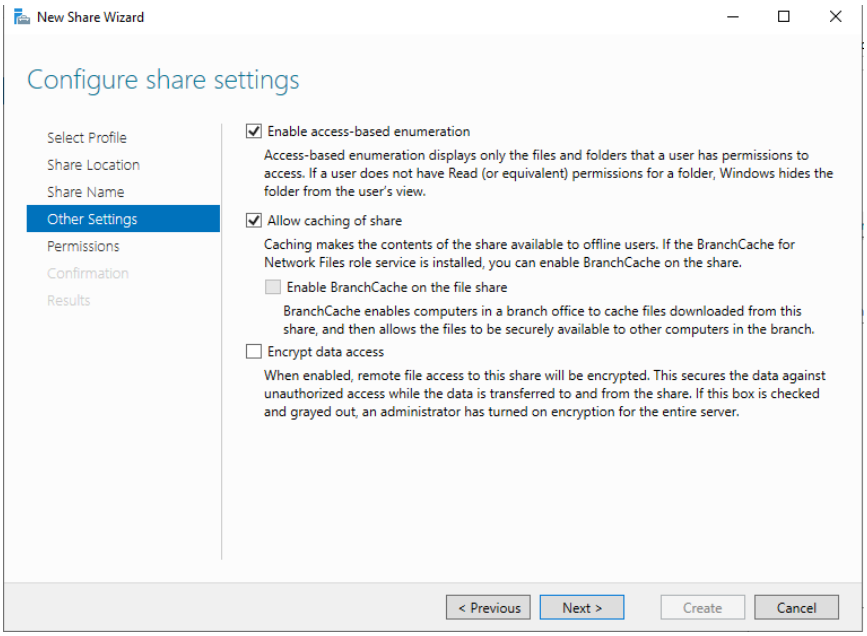

Slika 34: Putanja mape

Nakon toga je potrebno specificirati dijeljeno ime mape. Na kraju imena mape dodaje se znak $ što znači da će ta mapa biti skrivena od korisnika, odnosno neće im biti vidljiva. Kopira se Remote path to share (udaljenja putanja dijeljene mape na mreži) što će biti potrebno u sljedećim koracima, (slika 35.).



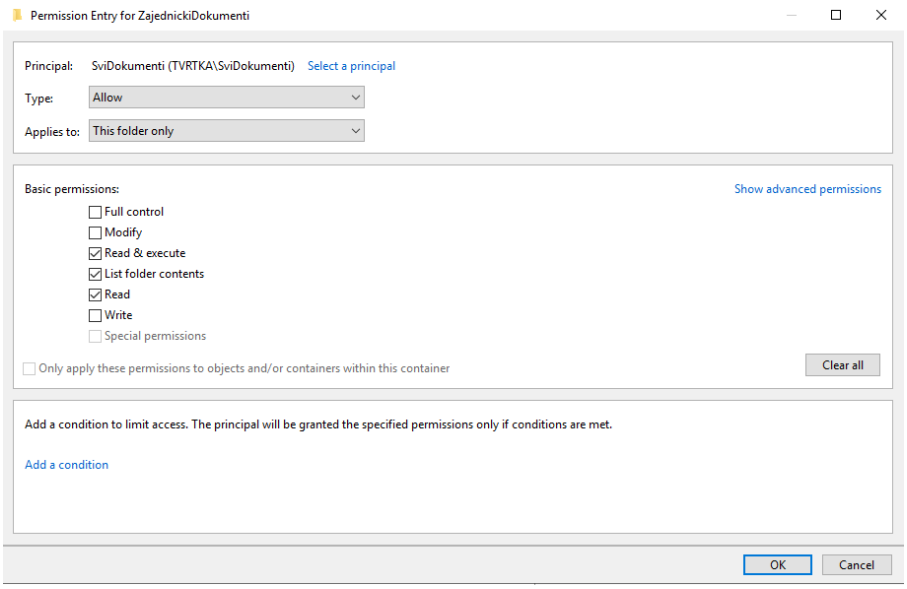

Slika 35: Specifikacija imena mape

U sljedećem koraku moramo još odrediti opciju Enable access-based enumeration koja znači ako korisnik nema dozvolu za čitanje (eng. *Read*) za tu mapu, Windows sakrije mapu od tog korisnika, (slika 36.).

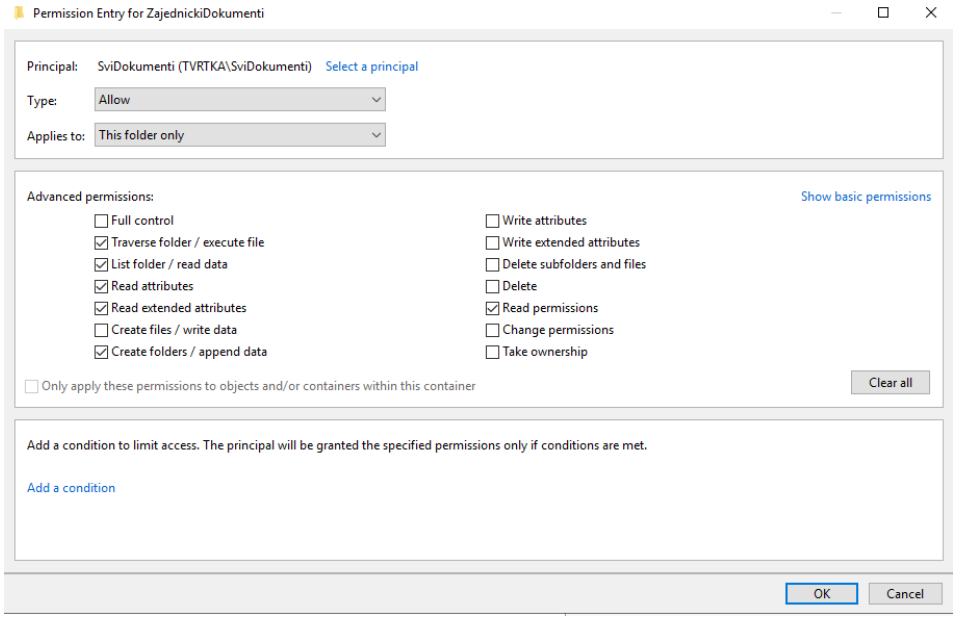



Slika 36: Konfiguracija dijeljenih opcija

Sada je potrebno dodati dozvolu za tu mapu za određenu grupu. Prije je kreirana grupa naziva SviDokumenti čiji su članovi radnici odjela Kadrovska. Oni će dobiti pristup ovoj mapi sa pripadajućim ovlastima vidljivima na slikama 37. i 38.

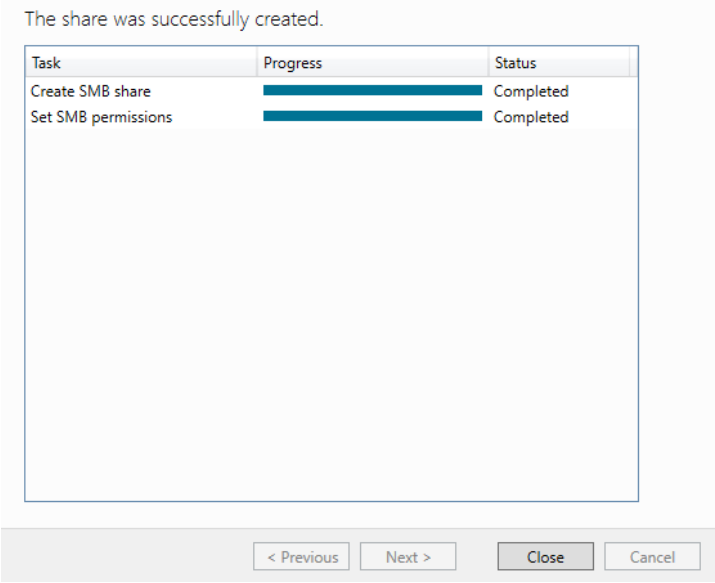



Slika 37: Dozvole



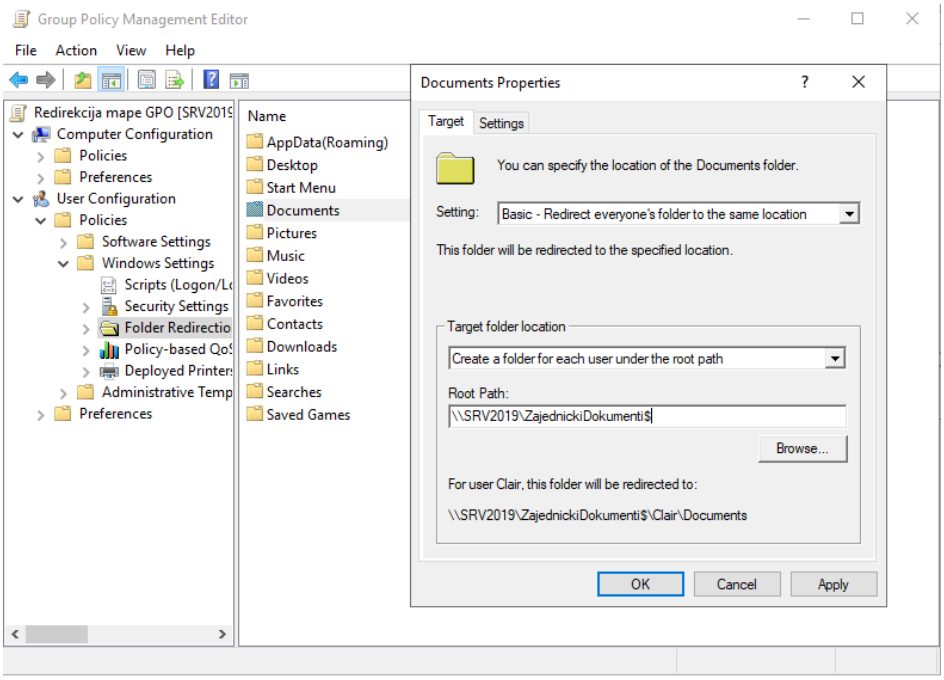

Slika 38: Temeljne dozvole

Dalje treba kreirati dijeljenje do kraja, (slika 39.).



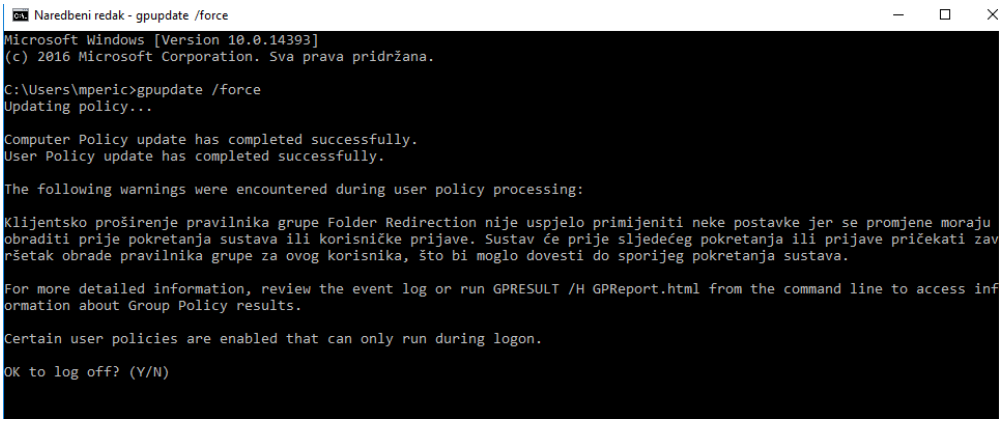

Slika 39: Završeno dijeljenje

Kreiramo novi GPO pod nazivom Redirekcija mape GPO te u Group Policy Management konzoli pod User Configuration\Policies\Windows Settings\Folder Redirection kopiramo putanju od mape, (slika 40.).



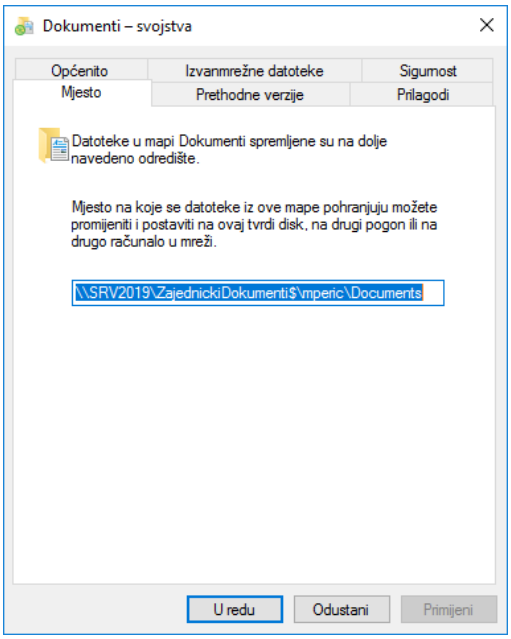

Slika 40: Svojstva dokumenata

Sada se prebacujemo na korisničko računalo, u Comand Promtu pokrećemo gpupdate /force te odjavljujemo korisnika i ponovo prijavljujemo kako bi se promjene izvršile, (slika 41.).




Slika 41: Command Prompt

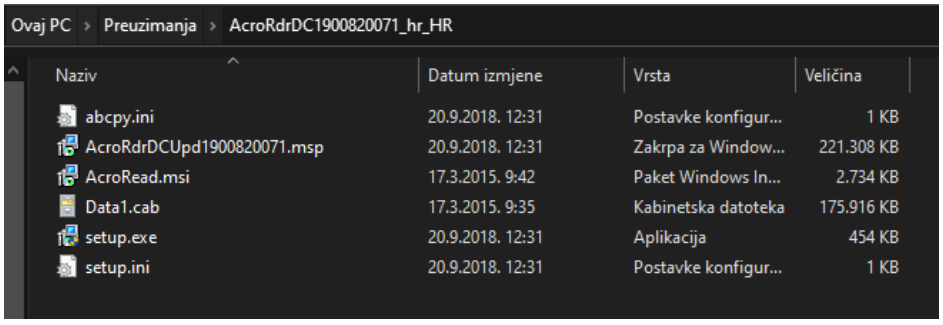
Promjene su se uspješno izvršile. Dokumenti za korisnika mperic će se preusmjeravati u mapu koja se nalazi na mrežnom mjestu: \\SRV2019\ZajednickiDokument$\mperic\Documents, (slika 42.).




Slika 42: Uspješno preusmjeravanje mape Dokumenti

## 4.5. Instalacija programa na računalo

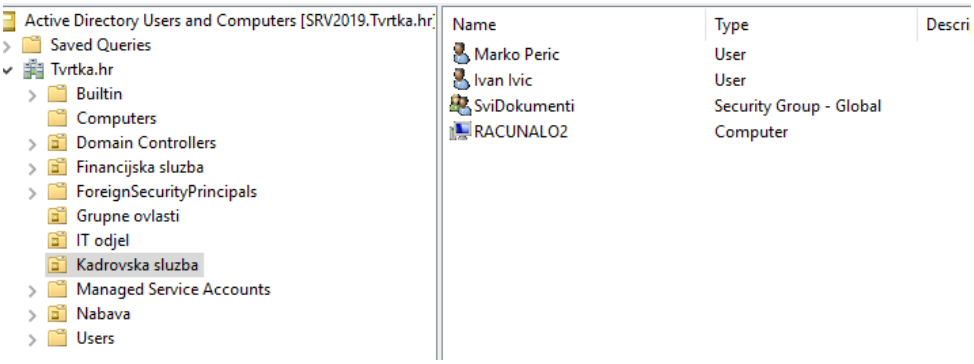
U ovom primjeru ću pokazati kako se na daljinu instalira neki program na računalo. Odabrala sam instalaciju Adobe Acrobat Reader-a, program za čitanje dokumenata u pdf formatu. Prvo je potrebno skinuti verziju instalacijske datoteke za Adobe Reader. Nakon toga treba tu datoteku raspakirati u mapu AcroRdr1900820071_hr_HR pomoću programa 7-Zip. Tim postupkom se dobiva datoteka ekstenzije msi koja je potrebna da bi se instalacija programa provela putem Group Policy. Ta datoteka je instalacijski paket Windowsa (Windows Instaler packages) i njezina ekstenzija znači Medium Scale Integration – razina ugrađenih tranzistora u mikročipu, (slika 43.).




Slika 43: Mapa AcroRdrDC1900820071_hr_HR

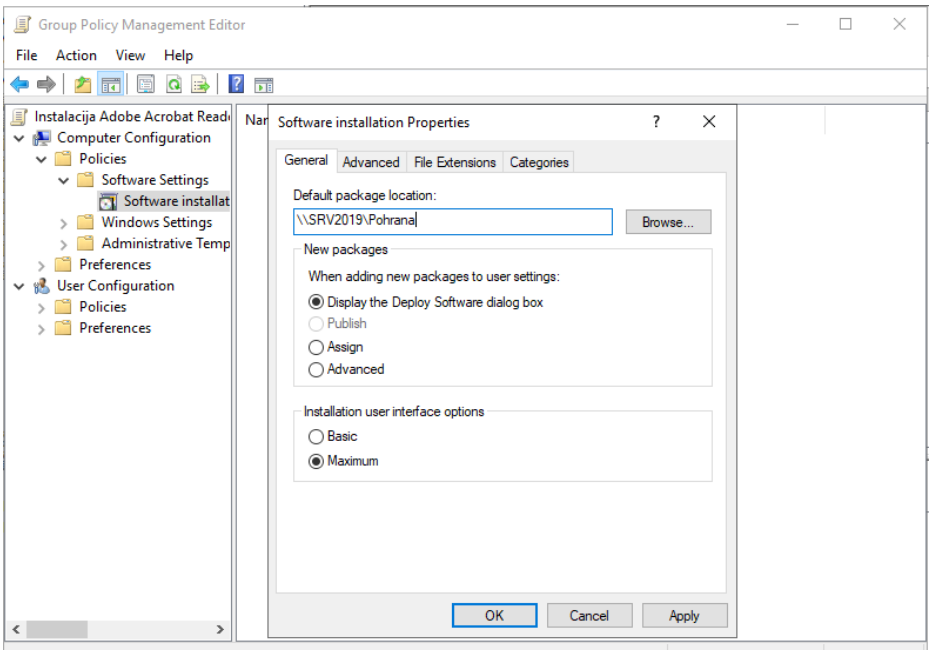
Mapu ACRORdc1900820071_hr_HR sam pospremila u mapu koju sam kreirala pod nazivom Pohrana na disku servera koju treba proglasiti da je dijeljena sa svim korisnicima.

Sljedeći korak je u Active Directory premjestiti računalo u odjel na koji će se primijeniti GPO. U našem slučaju je to odjel Kadrovska u kojem imamo dva korisnika, (slika 44.).



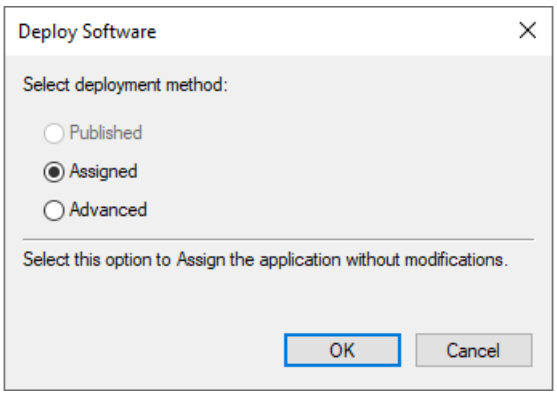

Slika 44: Odjel Kadrovska

U Group Policy Management kreira se nova GPO pod nazivom Adobe Acrobat Reader GPO. U Group Policy Management Editoru postavljamo zadnje postavke. Kopira se putanja od mape na serveru gdje je pospremljena instalacijska datoteka i primjenjuje se zadano, (slika 45.).



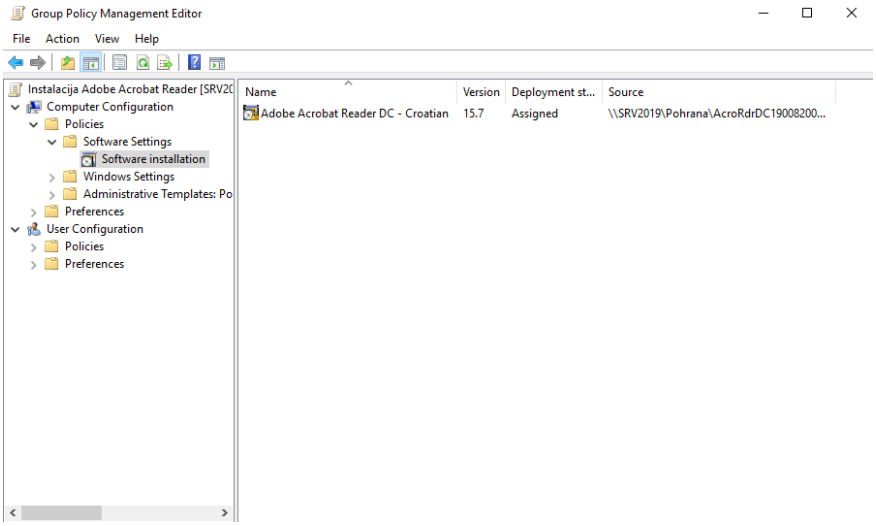

Slika 45: Group Policy Management Editor

Nakon toga je potrebno rasporediti program pomoću metode raspoređivanja sa opcijom *Assigned* što znači da će instalacija početi prilikom paljenja računalo, (slika 46.).



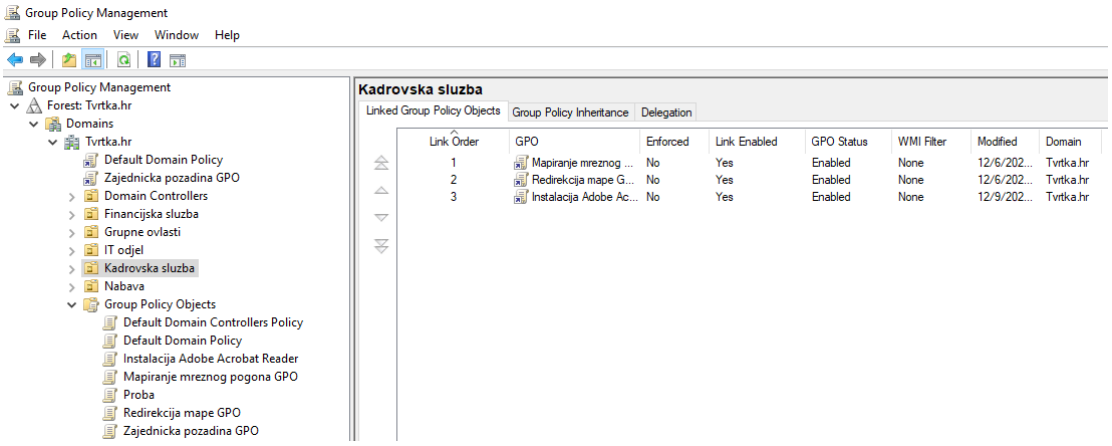

Slika 46: Metoda raspoređivanja

Uspješno je izvršeno raspoređivanje programa, (slika 47.).



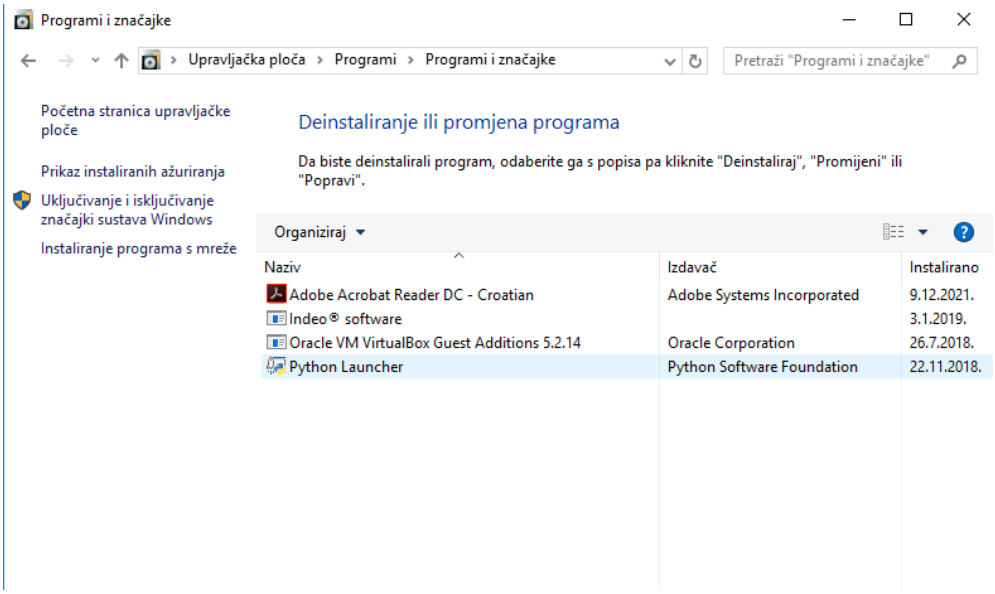

Slika 47: Raspoređivanje programa

Slijedeće je potrebno povezati GPO sa odjelom Kadrovska u koji je premješteno računalo, (slika 48.).




Slika 48: Povezana GPO u odjel Kadrovska

Sada je potrebno otići na klijentsko računalo i u ComandPromtu pokrenuti gpupdate /force, te odjaviti korisnika i ponovo prijaviti kako bi se promjene primijenile, odnosno provela instalacija programa. Nakon navedenog slijedi provjera da li su se pravila GPO-a primijenila na računalo. Na slici 49. vidljiva je provedena instalacija.

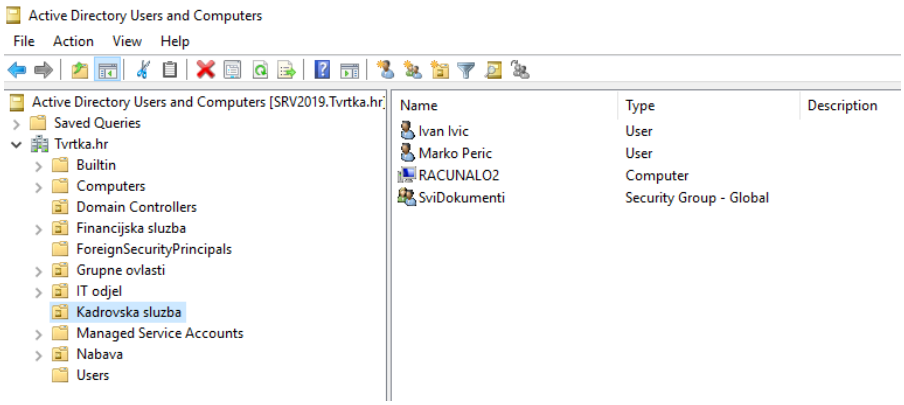



Slika 49: Provedena instalacija programa

Ovo pravilo Group Policy je kreirano na nivou konfiguracije računala što znači da će se primjenjivati na to računalo za svakog korisnika koji će se eventualno prijaviti na njega.

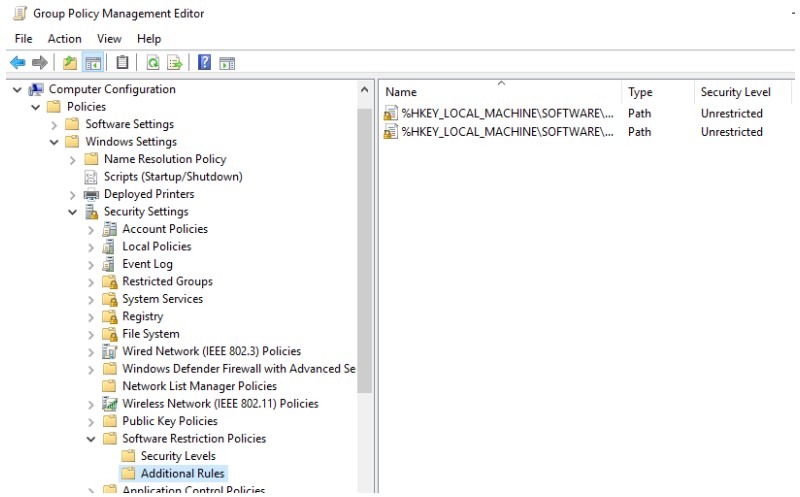
## 4.6. Onemogućen pristup određenim programima na računalu

Recimo da želimo na računalima ograničiti pristup korisnicima određenim programima. Ovaj primjer spada pod prevenciju sigurnosnih postavki. Za početak je potrebno računala na kojima želimo provesti ograničenja smjestiti u određenu organizacijsku jedinicu (odjel). U našem primjeru će to biti odjel Kadrovska, (slika 50.).



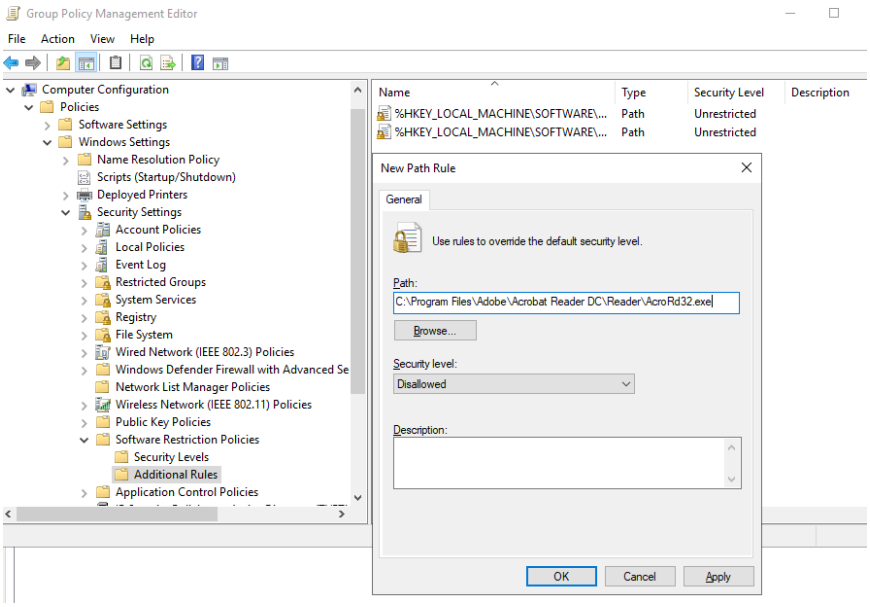

Slika 50: Odjel Kadrovska

U odjelu Kadrovska je jedno računalo naziva Racunalo2 na kojem ćemo pomoću Group Policy onemogućiti pristup programu Adobe Reader bilo kojem korisniku koje će se prijaviti na isti jer ćemo pravilo definirati na nivou konfiguracije računala. U Group Policy Managementu Editor-u ćemo kreirati novu GPO naziva *Onemogucen pristup programu Adobe GPO*. U uređivanju GPO-a idemo na konfiguraciju računala slijedećim redom: Computer Cofiguration\Policies\Windows Settings\Security Settings\Software Restriction Policies\Additional Rules, (slika 51.).



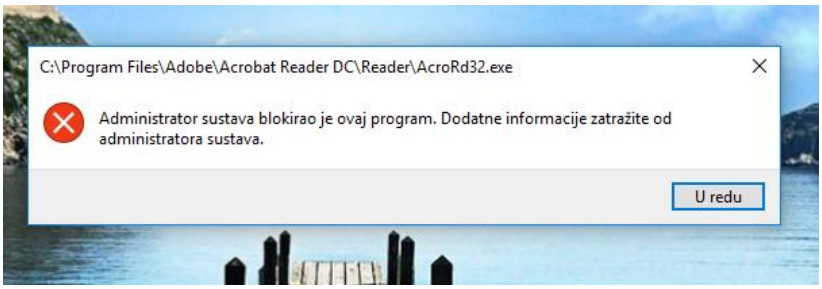

Slika 51: Group Policy Management Editor

Kreiramo novo pravilo, odnosno ubacujemo putanju na kojoj se nalazi instalirani program na računalu. Programi su u pravilu instalirani na računalima na sistemskoj particiji diska pod Program Files. Pod Security level mora biti odabrano Disallowed što znači nedopušteno pristupanje, (slika 52.).




Slika 52: Kreiranje pravila

Nakon toga potrebno je pokrenuti gpupdate i ponovo pokrenuti računalo u Comand Promtu kako bi se pravilo primijenilo. Nakon navedenog idemo testirati da li nam Group Policy radi tako da se prijavimo na računalo Racunalo2 kao korisnik i pokušamo otvoriti program Adobe Reader. Vidimo da nije moguće pokrenuti program i zaključujemo da smo ispravno kreirali pravilo, (slika 53.).




Slika 53: Provjera pravila Group Policy

# 5. Zaključak

Danas svaka tvrtka, bila mala ili velika teži funkcionalnom i sigurnom poslovnom sustavu. Da bi se navedeno moglo ostvariti potrebno je poduzeti niz koraka. Dio tih koraka je pravilno i sigurno upravljanje informacijskim sustavom u čemu bi trebale sudjelovati obrazovane i stručne osobe. U ovom radu je obrađeno sigurno administriranje sustava uz poštivanje sigurnosne politike. Ta politika, koja je sastavni dio sustava, iziskuje njegovu dobru organizaciju, rukovođenje važnim odlukama, usmjeravanje i educiranje zaposlenika u njihovim zadacima i rukovanju samom računalnom opremom i povjerljivim podacima. Jasno se trebaju definirati prihvatljivi i neprihvatljivi načini ponašanja kao i sankcija u slučaju nepridržavanja istih. Nadzor nad sustavom je među glavnim dijelovima upravljanja sigurnošću i obuhvaća osiguranje integriteta i dostupnosti informacija, provjera korištenja sustava da li je u skladu sa zahtjevima sigurnosne politike, nadzor nad radom ovlaštenih osoba, provođenje istrage u slučaju sumnje na sigurnosni incident te njegovo rješavanje.

Sudionici sustava su korisnici i davatelji usluga. Korisnici su oni koji se služe računalom u svojem radu i provode određene poslovne radnje. Davatelji informatičkih usluga su profesionalne osobe koje vode brigu o radu računala, mreže i cijelog sustava. Drugim riječima oni su specijalisti čiji je zadatak ukupna briga o sigurnosti sustava.

Administratori sustava ili domenski administratori nadziru domenski sustav, dodjeljuju korisnicima lozinke i ovlasti pristupa mrežnim resursima. Nadzor sustava administratori vrše kroz upravljački servis na serveru naziva Active Directory koji omogućava upravljanje domenom, korisničkim računima, mrežnim uređajima, klijentskim računalima, mrežom i drugim resursima. Upravljanje pravilima u domeni uvelike olakšava upotreba Group Policy kao centralizirana konfiguracija postavki operacijskog sustava. Ona omogućuje primjenu pravila nad velikim brojem računala unutar jedne domene, s jedne centralne lokacije. Navedeno olakšava rad administratora jer u protivnom da se ne koristi bilo bi potrebno odlaziti od jednog do drugog računala i ručno konfigurirati postavke. Group Policy se uređuje u konzoli GPMC koja pruža razne mogućnosti. U ovom radu kroz primjere je vidljivo koje sve pogodnosti ima upotreba GP-a.

Primjer uređivanja prava pristupa nad grupama korisnika je proveden u Active Directory bez upotrebe Group Policy ali je vrlo učinkovit način upravljanja pristupom određenim resursima na mreži. Cilj ovog primjera je pokazati kako se funkcionalno i brzo mogu postaviti sigurnosne postavke. U velikim sustavima je jako važno odvojiti odgovornosti poslovanja odjela ili organizacijskih jedinica i zaposlenika u njima. Otvaranjem raznih sigurnosnih grupa unutar domene je jedan način da se postigne gore navedeno. Upotrebom Group Policy može se provesti mapiranje mrežnih mapa pomoću skripta koja omogućuje instant postavke korisniku prilikom

prijave na računalo. U praksi se pokazalo da pojedini zaposlenici u velikim sustavima ne barataju baš vješto sa prepoznavanjem lokacije spremanja dokumenta. U većini slučajeva pospremaju dokumente lokalno na računalo, što u pravilu nije tako velika greška, ali ponekad to može izazvati poteškoće. Te poteškoće su u smislu da zaposlenik slučajno obriše dokument ili se pojavi hardwerski kvar te ostanu bez nekog važnog dokumenta. Tu uskače primjena GP-a kao dobro rješenje na način da se kreira pravilo koje sve dokumente preusmjerava i posprema na neku mrežnu mapu na serveru koja će se svakodnevno backupirati, te će se moći u svakom trenutku vratiti. Važno je napomenuti u ovom primjeru da korisniku nije vidljivo to preusmjeravanje. Onemogućavanje pristupa određenim programima na računalu je isto jedno od sigurnosnih postavki koja se pokazala kao dobro rješenje. Instalacija programa pomoću GP-a na veći broj računala skraćuje vrijeme koje bi bilo potrebno da se na svako računalo vrši instalacija pojedinačno. GP se može postaviti na nivou konfiguracije računala što znači prilikom paljenja računala i prijavom bilo kojeg ovlaštenog korisnika sustav postavlja zadane postavke. Kada je definirano pravilo na razini neke organizacijske jedinice, kod svih korisnika i računala u toj jedinici će se primjenjivati to pravilo. Na nivou korisničkog računa pravilo radi na način da se korisnik može prijaviti na bilo koje računalo u domeni i postavke tog računa će biti uvijek iste.

Mogu zaključiti da se primjena sigurnosnih pravila pomoću AD-a i GP-a pokazala kao dobra praksa u smislu brzog i točnog upravljanja i nadzora sustava. Takav način kao rezultat daje visoku razinu sigurnosti i zaštite poslovanja te podataka. Dio znanja za ovaj rad prikupila sam u svojoj radnoj praksi, dio istraživanjem i proučavanjem raznolike literature, a ostatak kroz praktični rad.

# 6. Literatura


1. Microsoft Server 2019 security aspects settimgs for small and medium-sized enterprises, Oleg Šimić, Listopad 2020.g., preuzeto 01.07.2022. s https://www.researchgate.net/publication/347962602_MICROSOFT_SERVER_2019_SECURITY_ASPECTS_SETTINGS_FOR_SMALL_AND_MEDIUM-SIZED_ENTERPRISES
2. Osnove administracije operacijskog sustava na poslužitelju (Windows server), priručnik za polaznika, Srce 2019.g., preuzeto 01.07.2022. s https://www.srce.unizg.hr/obrazovni-programi-za-it-specijaliste/obrazovni-program-za-it-specijaliste-edu4it/razina-sistemski-administrator-1/podrucje-windows/osnove-0
3. Active Directory Domain Services, preuzeto 12.07.2022. s https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services
4. DNS Overview, preuzeto 12.07.2022. s https://docs.microsoft.com/en-us/windows/win32/dns/dns-overview
5. What are Windows Security Policies?, ManageEngine, preuzeto 20.07.2022. s https://www.manageengine.com/products/desktop-central/windows-security-policies.html
6. Group Plicy Basics – Part 1: Understanding the Structure of a Group Policy Object, preuzeto 01.08.2022. s https://docs.microsoft.com/hr-hr/archive/blogs/musings_of_a_technical_tam/group-policy-basics-part-1-understanding-the-structure-of-a-group-policy-object
7. Group Policy Basic – Part 2: Understanding Which GPOs to Apply, preuzeto 01.08.2022. s https://docs.microsoft.com/hr-hr/archive/blogs/musings_of_a_technical_tam/group-policy-basics-part-2-understanding-which-gpos-to-apply
8. Group Policy Basic – Part 3: How Clients Proces GPOs, preuzeto 01.08.2022. s https://docs.microsoft.com/hr-hr/archive/blogs/musings_of_a_technical_tam/group-policy-basics-part-3-how-clients-process-gpos
9. Group Policy – Uvod, preuzeto 01.08.2022. s https://sistemac.srce.hr/node/98
10. Group Policy Object (GPO) auditing guide, ManageEngine ADAudit Plus, 02.08.2022. s https://www.manageengine.com/products/active-directory-audit/guide-to-configure-group-policy-object-auditing-in-adauditplus.html
11. Top 10 Most Important Group Policy Settings for Preventing Security Breaches, Lepide – Data Security, Danny Murphy, 10.07.2021.g., preuzeto 10.08.2022. s https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/

12. Sigurnosna politika informacijskih sustava za članice CARNeta (prijedlog), Hrvatska akademske i istraživačka mreža – CARNet, prosinac, 2003., Srce, Sveučilište u Zagrebu, preuzeto 10.08.2022. s http://sistemac-arhiva.srce.hr/index.php%3Fid%3Dsigurnost-ustanove.html
13. What are the GPC and the GPT?, Global Guideline, preuzeto 15.08.2022.g. s https://www.globalguideline.com/interview_questions/Answer.php?a=What_are_the_GPC_and_the_GPT_Where_can_I_find_them
14. Group Policy Management Console, preuzeto 15.08.2022. s https://docs.microsoft.com/en-us/previous-versions/windows/desktop/gpmc/group-policy-management-console-portal
15. Audit User Account Management, 15.08.2022. s https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-user-account-management
16. Change Windows Desktop Backround Using Group Policy, 15.08.2022. s https://www.mustbegeek.com/change-windows-desktop-background-using-group-policy/
17. Windows Active Directory i Group Policy , Igor Hitrec, Srce, 15.08.2022. s https://sysportal.carnet.hr/system/files/AD_GP.pdf
18. What is Windows Server and How Is It Different From Windows, MUO, preuzeto 15.08.2022. s https://www.makeuseof.com/tag/windows-server-different-windows/
19. What is Active Directory and how does it work?, TechTarget, preuzeto 15.08.2022. s https://www.techtarget.com/searchwindowsserver/definition/Active-Directory
20. Group Policy Managrmrnt Console, preuzeto 15.08.2022. s https://docs.microsoft.com/en-us/previous-versions/windows/desktop/gpmc/group-policy-management-console-portal

# 7. Popis slika