Primjena sigurnosnih politika u Windows domeni

Dolenec, Ana

Undergraduate thesis / Završni rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:407978

Rights / Prava: <u>Attribution-NonCommercial-NoDerivs 3.0 Unported/Imenovanje-Nekomercijalno-Bez</u> prerada 3.0

Download date / Datum preuzimanja: 2024-09-21



Faculty of Organization and Informatics - Digital Repository

Repository / Repozitorij:





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.

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.	Uv	od 1	
2.	Sig	gurnosna politika Windows domene2	
2	2.1. C	Organizacija upravljanja sigurnošću	2
	2.1	.1. Upravljanje mrežom	4
	2.1	.2. Sigurnosni incidenti	4
2	2.2. V	Vindows 10 domena	5
3.	Wi	ndows server 2019 i konfiguracija domenskog sustava	
3	8.1.	Active Directory	9
3	8.3.	Group Policy	0
	3.3	.1. Group Policy u ulozi sprečavanja sigurnosnih ispada1	1
	3.3	.2. Group Policy Management Console (GPMC)	1
4.	Pra	aktični dio – primjena sigurnosnih pravila u Windows domeni	
4	l.1.	Grupe korisnika i prava pristupa1	3
4	l.2.	Promjena slike pozadine na računalima1	5
2 r	l.3. ačur	Mapiranje mrežne mape pomoću skripte prilikom prijavljivanja korisnika na nalo2	2
2	I.4.	Preusmjeravanje mapa2	7
4	1.5.	Instalacija programa na računalo3	2
4	l.6.	Onemogućen pristup određenim programima na računalu	6
5.	Zal	ključak	
6.	Lite	eratura	
7.	Ро	pis slika	

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.).

Dashboard	erver Manager + L			• (3) r <u>1</u>	Manage	TASKS
Local Server All Servers AD DS	Active Directory Domain Service	es Configuration Wizard			TARGET SERVE	X load updates or IP
File and Storage	Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select the deployment operatio Add a domain controller to a Add a new domain to an exi Add a new forest Specify the domain information Root domain name: More about deployment config	n an existing domain titing forest for this operation Turtka.hr			ime Protection ps 01:00) Sarajevo ctivated Ryzen 5 3550H GB TASKS •

Slika 2: Kolekcija domena

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

<u>ج</u> ب	Server Manager + Lo	ocal Server	• © P	Manage Tools	View Help
 Dashboard Local Server All Servers AD DS DNS File and Storage 	Active Directory Domain Service Domain Controlled Deployment Configuration Domain Controlled Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	TIES 19 Is Configuration Wizard I Options Select functional level of the new for Forest functional level: Domain functional level: Specify domain controller capabiliti I Domain functional level: Specify domain controller capabiliti I Clobal Catalog (GC) Read only domain controller (R Type the Directory Services Restore Password: Confirm password:	es verst and root domain Windows Server 2016 v Windows Server 2016 v es rver ODC) Mode (DSRM) password ••••••••	- C X	TASKS TASKS TASKS TASKS TASKS TASKS TASKS T
	SRV2019 8	198 Error Microsoft-Windows-S	< Previous Next > Insta Security-SPP Application	II Cancel	

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

📓 Group Policy Management 📓 File Action View Window Help				
🗢 🔿 🙍 🛅 🕒 İ 🗙 🙆 🛛 🖬				
Image: Group Policy Management ✓ ▲ Forest: I/vtka.hr ✓ ▲ Domains ✓ A Domains ✓ ▲ Domains <td< td=""><td>Onemogucen pristup pro Scope Details Settings Delega Links Display links in this location: The following stee, domains, and O</td><td>gramu Adobe GPO tion Status Tvrtka.hr Us are linked to this GPO:</td><td></td><td></td></td<>	Onemogucen pristup pro Scope Details Settings Delega Links Display links in this location: The following stee, domains, and O	gramu Adobe GPO tion Status Tvrtka.hr Us are linked to this GPO:		
 > @ Dormain Controllers > @ Financijska sluzba > @ Grupne ovlasti > @ Todjel > @ Kadrovska sluzba > @ Nabava > @ Group Policy Objects @ Default Domain Policy @ Instalacija Adobe Acrobat Reader Mapizna Adobe upristup programu Adobe Onemogucen pristup programu Adobe Proba 	Location	Enforced No	Link Enabled Yes	Path Tvrtka hr/Kadrovska sluzba
Zeječnickcija mape GPO Zeječnicka pozadina GPO Zeječnicka pozadina GPO Site Sites GPOs Group Policy Modeling Group Policy Results	Security Filtering The settings in this GPO can only ap Name & Authenticated Users	oply to the following groupe, u	sers, and computers	
< >>	Add Rer WMI Filtering This GPO is linked to the following crosne>	nove Propertie WMI filter:	s Open	

Slika 6: Group Policy Management Console

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.

 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.).

Ivan Ivic Properties				? X			Ivan Ivic Pro	perties				?	×
Remote control	Bemote	Desktop Se	ervices Profile	COM+			Remote of	ontrol	Remote	Desktop S	ervices Profile	0	OM+
General Address	Account	Profile	Telephones	Organization	Select Groups	х	General	Address	Account	Profile	Telephones	Organ	nization
Member Of	Dial-in	Env	ironment	Sessions			Member	Of	Dial-in	En	vironment	Sess	ions
Member of:					Select this object type:		Member of:						
News	Anti-	Denei	Constant Folder		Groups or Built-in security principals	Object Types	Name		Active Direct	ony Domai	n Services Folde	r	
Name	T d L dl	tory Domain	1 Services Poide	D:	From this location:		Domain I	leare	Tyrtka br/l k	are			
SviDokumenti	Tvrtka.hr/Us	sers drovska sk	izha		Tvrtka.hr	Locations	Financije	RW	Tvrtka.hr/Gr	upne ovlas	si		
ononanana	1100030710				Enter the object names to select (examples):		SviDokur	nenti	Tvrtka.hr/Ka	drovska sl	uzba		
					Advanced	OK Cancel							
Add	Remove						Add	ł	Remove				
Primary group: E	Iomain Users						Primary gro	up: D	omain Users				
Set Primary Group	There is you have application	no need to Macintosh ons.	change Primary clients or POSI	group unless K-compliant			Set Prim	ary Group	There is a you have application	no need to Macintosh ns.	change Primary n clients or POS	group ur X-complia	iless ant
C	К	Cancel	Apply	Help			1	0	K	Cancel	Apply		Help

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.).

			Financije RW Proper	ties	?	×
Financije RW Properties ? X	1		General Members	Member Of Managed By		
General Members Member Of Managed By	Select likers Contacts Computers Senire Accounts or Groups	×	Name	Active Directory Domain Services Fold	ər	
Members: Name Active Directory Domain Services Folder	Select this object type:		& Ana Dolenec & Ivan Ivic	Tvrtka.hr/IT odjel Tvrtka.hr/Kadrovska sluzba		
💑 Ana Dolenec 🛛 Tvrtka.hr/lT odjel	Users, Service Accounts, Groups, or Other objects From this location:	Object Types				
	Tvttka hr Enter the object names to select (<u>examples</u>): [<u>van lvtc (ivtc@Tvtka hr</u>]	Locations Check Names				
	Advanced OK	Cancel				
Add Remove			Add	Remove		
OK Cancel Apply				OK Cancel	A	pply

Slika 8: Dodavanje korisnika u grupu

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

arko Perio	c Propertie	s			?	×F	inanacij	e R Prope	rties					?	
Remote	control	Remote	Desktop Se	ervices Profile	CON	4+	General	Members	Member O	f 1	lanane	d By			
General	Address	Account	Profile	Telephones	Organiz	ation	General	1000000	Member of		lanage	u by			
Membe	er Of	Dial-in	Env	vironment	Session	15	Membe	rs:							
Member o	f:					_	Name		Active D)irec	tory Do	main S	Services F	older	
Name Domain	Users	Active Direct	tory Domair iers	n Services Folder	÷.		<u>&</u> M	arko Peric	Tvrtka.h	ir/Ki	idrovsk	a sluz	ba		
Finanaci	ije R	Tvrtka.hr/Gr	upne ovlas	ti											
SviDoku	umenti	Tvrtka.hr/Ka	idrovska sli	uzba											
Add.		Remove													
^o rimary gr	roup: D	omain Users	no need to	change Primary	aroup unles	55									
Set Prir	mary Group	you have applicatio	Macintosh ins.	clients or POSI	K-compliant	E.	Ac		Demana	-					
								id	Hemove						

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.).

🕌 Server2019 [Running]] - Oracle VM VirtualBox			
File Machine View	Input Devices Help			
🏪 🛛 🛃 📙 🖛 🛛 Local Disk (C	C:)			
File Home Share	View			
\leftarrow \rightarrow \checkmark \uparrow 🏪 \flat This	s PC → Local Disk (C:)			
	Name	Date modified	Туре	Size
Quick access		12/3/2021 10:35 AM	File folder	
Desktop 🖌	PerfLogs	9/15/2018 9:19 AM	File folder	
Uownloads 🖈	Program Files	12/1/2021 8:47 PM	File folder	
🔮 Documents 🛛 🖈	Program Files (x86)	12/1/2021 8:44 PM	File folder	
📰 Pictures 🛛 🖈	Users	12/1/2021 12:28 PM	File folder	
🏪 Local Disk (C:) 📝	Windows	12/3/2021 9:43 AM	File folder	
ZajednickaPozac 🖈	📙 ZajednickaPozadina	12/6/2021 1:21 PM	File folder	
💻 This PC	ZAJEDNICKI DOKUMENTI	12/3/2021 10:25 AM	File folder	
💣 Network				

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

Permissions for ZajednickaPo	zadina	×
Share Permissions		
Group or user names:		
Serveryone		
	Add	Remove
Permissions for Everyone	Allow	Deny
Permissions for Everyone Full Control	Allow	Deny
Permissions for Everyone Full Control Change Band		Deny
Permissions for Everyone Full Control Change Read	Allow	Deny
Permissions for Everyone Full Control Change Read	Allow	
Permissions for Everyone Full Control Change Read	Allow	Deny
Permissions for Everyone Full Control Change Read		Deny
Permissions for Everyone Full Control Change Read		Deny

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.).

ZajednickaPozadina Properties	×
General Sharing Security Previous Versions Customize	
Network File and Folder Sharing Zajednicka Pozadina Shared Network Path: (\SRV2019\ZajednickaPozadina	
Share Advanced Sharing Set custom permissions, create multiple shares, and set other advanced sharing options.	
Close Cancel Apply	

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.).

器 Server2019 [Run	ning] - Oracle VM VirtualBox	
File Machine Vi	ew Input Devices Help	
Group Policy Manage	ement / Window Help	
Group Policy Manag Composed Angle A	ement Tvrtka.hr Status Linked Group Policy Objects	Gro
✓ jiji Tvrt' ' 30 31 32 32 33 31	Create a GPO in this domain, and Link it here Link an Existing GPO Block Inheritance	Dire
	Group Policy Modeling Wizard New Organizational Unit	ne ba
> 1 > 1 > 1 > 1 > 1 > 1 S 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 =	Search Change Domain Controller Remove Active Directory Users and Computers	exist
🔂 Group F	View >	
	Refresh Properties	
	Help	

Slika 14: Kreiranje GPO na razini domene

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

New GPO	×
Name:	
Zajednicka pozadina GPO	
Source Starter GPO:	
(none)	~



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.).



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 (<u>\\SRV2019\ZajednickaPozadina\Pozadina.png</u>), (slika 17.).

Desktop Wallpaper	- 0	×
🛅 Desktop Wallpaper	Previous Setting Next Setting	
O Not Configured Comment:		^
Enabled		
O Disabled Supported on:	east Windows 2000	~ ~
Options:	Help:	
Wallpaper Name: [\\SRV2019\Zajednicka Example: Using a local path: C\windows\web\wallpaper\home.jpg Example: Using a UNC path: \\Server\Sh Wallpaper Style: Fill ~	zadina\Pozadini Specifies the desktop background ("wallpaper") displayed on all users' desktops. \Corp.jpg This setting lets you specify the wallpaper on users' desktops and preve users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (".bmp) or JPEG (".jpg) file. To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C: Windows/web/wallpaper/homejap or 2 UNC path, such as \Cserver \Share\Corp.jpg. If the specified file is not available when the user logs no wallpaper is displayed. Users cannot specify alternative wallpaper, 't can also use this setting to specify that the wallpaper image be centered tide, or stretched. Users cannot change this specification. If you disable this setting or do not configure it, no wallpaper is displayed. However, users can select the wallpaper of their choice. Also, see the "Allow only bitmapped wallpaper" in the same location, a	n, u d.

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.).

POČETNI IZBORNIK	Letimičan pogled i	na život		lgra i istraživanje			
	je <mark>ponedjeljak</mark>	Govorin [.] Pošta	no Gmail	Xbox	Groove glazba	Filmovi i TV	
	C Microsoft Edge	Fotografije	$\overline{\uparrow}$	$\overline{\uparrow}$	$\overline{\mathbf{A}}$	$\overline{\uparrow}$	
	Skype Preview	$\overline{\uparrow}$	$\overline{\uparrow}$	$\overline{\uparrow}$	\pm	$\overline{\uparrow}$	
	u ~	à	$\overline{\uparrow}$	$\overline{\uparrow}$	L Nabavite Office	OneNote	
8 Marko Peric							
Ø Postavke							
🖒 Uključi/isključi							12.44

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.).

Group Policy Management Editor File Action View Help		-		\times
Mapiranje mreznog pogona GPO [SRV2019.TVRTKA.HR] Policy Me Computer Configuration Policies Preferences Me Configuration	Scripts (Legon/Logoff) Logon Name Display Properties Cogon Logoff			
 Policies Software Settings Windows Settings Scripts (Logon/Logoff) Security Settings Folder Redirection Ipolicy-based QoS 	Clogon Properties Scripts PowerShell Scripts Logon Scripts for Mapirarje mreznog po	ogona GP	?	×
 > Deployed Printers > Administrative Templates: Policy definitions (ADMX fil > Preferences 	Name Parameters		Up Down Add Edit Remove	
< >	To view the script files stored in this Group Policy O the button below.	bject, pres	35]	ły

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.).

File Machine V	iew	Input Devices	нер						
🔒 🛃 📑 🖛 l Logo	n								
File Home	Share	View							
	> Ne	twork > Tvrtka.hr >	SysVol >	Tvrtka.hr → Poli	cies > {00957AB9-133	3-4513-B208-3E11401A	6E7F} > User	Scripts	⇒ Logon
		Name	^		Date modified	Туре	Size		
📌 Quick access		💿 map.bat			12/6/2021 5:41 PM	Windows Batch File	1 KB		
Desktop	*								
👆 Downloads	*								
Documents	1								
Pictures	*								
🏪 Local Disk (C:)									
ZajednickaPoz	adina								
🔜 This PC									
🔿 Network									

Slika 27: Konzola GPO

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

Logon Properties			?	×
Scripts PowerShell Scripts				
Logon Scripts fo	r Mapiranje mrezi	nog pogona GPC)	
Name	Parameters	_		
map.bat			Up	
			Down	
			Add	
			Edit	
			Lon	
			Remove	
To view the script files stored the button below.	l in this Group Pc	licy Object, pres	\$	
	ОК	Cancel	Appl	y

Slika 28: Dodavanje skripte u GPO

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

Group Policy Management	Kadro	vska sluzba							
✓ A Forest: Tvrtka.hr	Linked	Group Policy Objects	Group Policy Inheritance	Delegation					
🗸 📑 Domains									
✓ jii Tvrtka.hr		Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
🗊 Default Domain Policy		1	Mapiranje mreznog	No	Yes	Enabled	None	12/6/202	Tvrtka.hr
🛒 Zajednicka pozadina GPO									
> 💼 Domain Controllers									
> 💼 Financijska sluzba	$\overline{\nabla}$								
> 💼 Grupne ovlasti									
> 🧰 IT odjel									
> 📓 Kadrovska sluzba									
> 📓 Nabava									
✓ Croup Policy Objects									
Default Domain Controllers Policy									
Default Domain Policy									

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.).

Server N Servers	lanager • File an	d Storage Services	 Shares 	TASKS VOLUME KORISNICI on
Volumes Disks Storage Pools Stares ISCSI Work Folders	Filter Filter Share Share SRV2019 (4) KORISNIC NETLGON SYSVOL ZajednickaPozadina	P B ● P New Share Wizard Select the profile Share Location Share Location Share Vame Other Settings Permissions Confirmation Results	for this share File share profile: SMB Share - Quick SMB Share - Applications NFS Share - Quick NFS Share - Quick NFS Share - Quick	Description: This basic profile represents the fastest way to create an Mindows-based computers. Suitable for general file sharing Advanced options can be configured later by using the Properties dialog
				< Previous Next > Create Cancel

Slika 33: New Tasks

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

elect Profile	Server:						
hare Location	Server Name	Status	Cluster F	lole	Owner Node		
hare Name	SRV2019	Online	Not Clus	tered			
ermissions							
	Share leasting						
	Share location:						
	Share location: Select by volume:	5 6	Constitu	File Casta			
	Share location: Select by volume: Volume	Free Space	Capacity	File System	1		
	Share location: Select by volume: Volume C:	Free Space 87.2 GB	Capacity 99.5 GB	File System NTFS	1		
	Share location: Select by volume: Volume C:	Free Space 87.2 GB	Capacity 99.5 GB	File System NTFS	1		
	Share location: Select by volume: Volume C:	Free Space 87.2 GB	Capacity 99.5 GB	File System	1		
	Share location: Select by volume: Volume C: The location of the final	Free Space 87.2 GB le share will be a new fol	Capacity 99.5 GB	File System NTFS hares direc	tory on the se	lected	
	Share location: Select by volume: Volume C: The location of the fir volume.	Free Space 87.2 GB le share will be a new fol	Capacity 99.5 GB Ider in the \SI	File System NTFS hares direc	tory on the sel	lected	

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.).

📥 New Share Wizard			-		×
Specify share nan	ne				
Select Profile	Share name:	ZajednickiDokumenti\$			
Share Location					
Share Name	Share description:				
Other Settings					
	Local path to share:				
	C:\ZajednickiDokur	nenti			
	Remote path to sha	re:			
	\\SRV2019\Zajedni	ckiDokumenti\$			
		< Previous Next > Crea	ate	Cancel	

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.

Permission	n Entry for ZajednickiDokumenti				×
Principal:	SviDokumenti (TVRTKA\SviDokumenti) Select a principal				
Туре:	Allow ~				
Applies to:	This folder only \lor				
Basic permi	ssions:	Show	advanced	1 permiss	ions
	Full control			1	
	☐ Modify				
	Read & execute				
	✓ List folder contents				
	Read				
	Write				
	Special permissions				
Only app	ly these permissions to objects and/or containers within this container			Clear al	I
Add a cond	ition to limit access. The principal will be granted the specified permissions only if conditions are met.				
Add a cond	ition				
			ОК	Can	cel

Slika 37: Dozvole

Permission	n Entry for ZajednickiDokumenti		- D ×
Principal:	SviDokumenti (TVRTKA\SviDokumenti) Select a princip	pal	
Туре:	Allow		
Applies to:	This folder only \checkmark		
Advanced p	permissions:		Show basic permissions
	Full control	Write attributes	
	Traverse folder / execute file	Write extended attributes	
	List folder / read data	Delete subfolders and files	
	Read attributes	Delete	
	Read extended attributes	Read permissions	
	Create files / write data	Change permissions	
	Create folders / append data	Take ownership	
🗌 Only app	ly these permissions to objects and/or containers within t	his container	Clear all
Add a cond	ition to limit access. The principal will be granted the spec	ified permissions only if conditions are met.	
Add a cond	ition		
			OK Cancel

Slika 38: Temeljne dozvole

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

Task	Progress	Status
Create SMB share		Completed
Set SMB permissions		Completed

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.).

Group Policy Management Editor			_		\times
File Action View Help					_
🗢 🌳 🖄 📰 🔚 🗟 🖬		Documents Properties	?	×	
Redirekcija mape GPO [SRV2015 Computer Configuration Policies Policies Software Settings Administrative Temp Preferences	Name AppData(Roaming) Desktop Start Menu Documents Pictures Nusic Videos Favorites Contacts Downloads Links Searches Saved Games	Target Settings You can specify the location of the Documents for Setting: Basic - Redirect everyone's folder to the same lo This folder will be redirected to the specified location. Target folder location [Create a folder location derived to the root path Root Path: [\SRV2019\ZajednickiDokumenti\$] For user Clair, this folder will be redirected to: \\SRV2019\ZajednickiDokumenti\$\Clain\Documents OK Cancel	lder. ation	▼ ▼	

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: <u>\\SRV2019\ZajednickiDokument\$\mperic\Documents</u>, (slika 42.).

Dokumenti – sv	rojstva	
Općenito	Izvanmrežne datoteke	Sigumost
Mjesto	Prethodne verzije	Prilagodi
Datoteke u r navedeno od	napi Dokumenti spremljene su na dredište.	dolje
Mjesto na ko promijeniti i p drugo računa	ije se datoteke iz ove mape pohra ostaviti na ovaj tvrdi disk, na drug alo u mreži.	anjuju možete ji pogon ili na
\\SRV2019	\ZajednickiDokumenti\$\mperic\[Documents

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.).

Ova	aj PC → Preuzimanja → AcroRdrDC19008200	71_hr_HR		
^	Naziv	Datum izmjene	Vrsta	Veličina
	👼 abcpy.ini	20.9.2018. 12:31	Postavke konfigur	1 KB
	🕼 AcroRdrDCUpd1900820071.msp	20.9.2018. 12:31	Zakrpa za Window	221.308 KB
	🕼 AcroRead.msi	17.3.2015. 9:42	Paket Windows In	2.734 KB
	📑 Data1.cab	17.3.2015. 9:35	Kabinetska datoteka	175.916 KB
	🙀 setup.exe	20.9.2018. 12:31	Aplikacija	454 KB
	🔊 setup.ini	20.9.2018. 12:31	Postavke konfigur	1 KB

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.).

Group Policy Management Editor			_	×
File Action View Help				
🗢 🄿 🙍 📷 🔯 😰	PE			
 Instalacija Adobe Acrobat Readi Computer Configuration Policies Software Settings Software installat Windows Settings Administrative Temp Preferences Policies Policies Policies Preferences 	Nar Software installation Properties General Advanced File Extensions Categories Default package location: \\SRV2019\Pohranal E \\SRV2019\Pohranal E When adding new packages to user settings: Image: Comparison of the setting of the s	? × Browse		
< >	Calcor	, which	1	

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.).

Deploy Software	×			
Select deployment method:				
O Published				
Assigned				
◯ Advanced				
Select this option to Assign the application without modifications.				
OK Cancel				

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.).

📓 Group Policy Management									
🖼 File Action View Window Help									
💠 🔿 🚾 🖸 🖬									
📓 Group Policy Management	Kadr	ovska sluzba							
✓ ▲ Forest: Tvrtka.hr	Linke	d Group Policy Objects	Group Policy Inheritance	Delegation					
🗸 📑 Domains				beiegenen					
✓ jii Tvrtka.hr		Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
Default Domain Policy		1	🛒 Mapiranje mreznog	No	Yes	Enabled	None	12/6/202	Tvrtka.hr
🛒 Zajednicka pozadina GPO	_	2	Redirekcija mape G	No	Yes	Enabled	None	12/6/202	Tvrtka.hr
> 📔 Domain Controllers		3	🛒 Instalacija Adobe Ac	No	Yes	Enabled	None	12/9/202	Tvrtka.hr
> 💼 Financijska sluzba									
> 🛅 Grupne ovlasti									
> 🛅 IT odjel									
> 📔 Kadrovska sluzba									
> 🛱 Nabava									
🗸 📑 Group Policy Objects									
Default Domain Controllers Policy									
Default Domain Policy									
🧾 Instalacija Adobe Acrobat Reader									
🧾 Mapiranje mreznog pogona GPO									
I Proba									
🧾 Redirekcija mape GPO									
🧾 Zajednicka pozadina GPO									

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. Onemoqućavanje 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

- Microsoft Server 2019 security aspects settings 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_SE CURITY_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 <u>https://www.srce.unizg.hr/obrazovni-programi-za-it-specijaliste/obrazovni-program-za-it-specijaliste-edu4it/razina-sistemski-administrator-1/podrucje-windows/osnove-0</u>
- Active Directory Domain Services, preuzeto 12.07.2022. s https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domainservices
- 4. DNS Overview, preuzeto 12.07.2022. s <u>https://docs.microsoft.com/en-us/windows/win32/dns/dns-overview</u>
- 5. What are Windows Security Policies?, ManageEngine, preuzeto 20.07.2022. s https://www.manageengine.com/products/desktop-central/windows-security-policies.html
- Group Plicy Basics Part 1: Understanding the Structure of a Group Policy Object, preuzeto 01.08.2022. s <u>https://docs.microsoft.com/hr-</u> <u>hr/archive/blogs/musings_of_a_technical_tam/group-policy-basics-part-1-understanding-</u> <u>the-structure-of-a-group-policy-object</u>
- Group Policy Basic Part 2: Understanding Which GPOs to Apply, preuzeto 01.08.2022. s <u>https://docs.microsoft.com/hr-hr/archive/blogs/musings_of_a_technical_tam/group-policy-basics-part-2-understanding-which-gpos-to-apply</u>
- 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/grouppolicy-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-configuregroup-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 <u>https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/</u>

- 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 <u>http://sistemac-arhiva.srce.hr/index.php%3Fid%3Dsigurnost-ustanove.html</u>
- 13. What are the GPC and the GPT?, Global Guideline, preuzeto 15.08.2022.g. s <u>https://www.globalguideline.com/interview_questions/Answer.php?a=What_are_the_GP</u> <u>C_and_the_GPT_Where_can_l_find_them</u>
- 14. Group Policy Management Console, preuzeto 15.08.2022. s <u>https://docs.microsoft.com/en-us/previous-versions/windows/desktop/gpmc/group-policy-management-console-portal</u>
- 15. Audit User Account Management, 15.08.2022. s <u>https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-user-account-management</u>
- 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 <u>https://www.makeuseof.com/tag/windows-server-different-windows/</u>
- 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 Managrmmt Console, preuzeto 15.08.2022. s https://docs.microsoft.com/en-us/previous-versions/windows/desktop/gpmc/group-policymanagement-console-portal

7. Popis slika

Slika 1: Domena (izradila autorica)	5
Slika 2: Kolekcija domena	7
Slika 3: Domain Controller Options	8
Slika 4: Local Server	8
Slika 5: Struktura u Active Directory Users and Computers	9
Slika 6: Group Policy Management Console	12
Slika 7: Dodavanje grupe korisniku	14
Slika 8: Dodavanje korisnika u grupu	14
Slika 9: Dodan korisnik u grupu Financije R	15
Slika 10: Mapa na disku servera	16
Slika 11: Dijeljenje mape	16
Slika 12: Određivanje ovlasti za mapu	17
Slika 13: Network Path	17
Slika 14: Kreiranje GPO na razini domene	18
Slika 15: Naziv GPO-a	18
Slika 16: Desktop	19
Slika 17: Desktop Wallpaper	19
Slika 18: Klijentsko računalo	20
Slika 19: Command Prompt (naredbeni redak)	20
Slika 20: Nova slika pozadine	21
Slika 21: Nemogućnost promjene slike pozadine kao korisnik	21
Slika 22: Dijeljena mapa	22
Slika 23: Bat datoteka	23
Slika 24: Mapirana mapa	23
Slika 25: Kreirana GPO	24
Slika 26: Logon opcija	24
Slika 27: Konzola GPO	25
Slika 28: Dodavanje skripte u GPO	25
Slika 29: Povezivanje GPO	25
Slika 30: Korisnici u Active Directory	26
Slika 31: Command Prompt	26
Slika 32: Mapirani mrežni pogon K	26
Slika 33: New Tasks	27
Slika 34: Putanja mape	28
Slika 35: Specifikacija imena mape	28
Slika 36: Konfiguracija dijeljenih opcija	29
Slika 37: Dozvole	29
Slika 38: Temeljne dozvole	30
Slika 39: Završeno dijeljenje	30
Slika 40: Svojstva dokumenata	31
Slika 41: Command Prompt	31
Slika 42: Uspješno preusmjeravanje mape Dokumenti	32
Slika 43: Mapa AcroRdrDC1900820071_hr_HR	32
Slika 44: Odjel Kadrovska	33
Slika 45: Group Policy Management Editor	33

Slika 46: Metoda raspoređivanja	. 34
Slika 47: Raspoređivanje programa	. 34
Slika 48: Povezana GPO u odjel Kadrovska	. 35
Slika 49: Provedena instalacija programa	. 35
Slika 50: Odjel Kadrovska	. 36
Slika 51: Group Policy Management Editor	. 36
Slika 52: Kreiranje pravila	. 37
Slika 53: Provjera pravila Group Policy	. 37