Porovnanie doménových radičov na systémoch Linux a Windows

Bc. Patrícia Mravcová

Diplomová práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Patrícia Mravcová**
Osobní číslo:	**A21813**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní technologie**
Forma studia:	**Kombinovaná**
Téma práce:	**Porovnání doménových řadičů na systémech Linux a Windows**
Téma práce anglicky:	**Comparison of Domain Controllers on Linux and Windows**

Zásady pro vypracování

1. Zpracujte teorii o počítačových sítích, operačních systémech a doménových řadičích.
2. Popište nasazení Microsoft Active Directory, připojení pracovních stanic, konfiguraci vybraných služeb a bezpečnostních politik.
3. Vyzkoušejte a popište nasazení obdobného systému na jiné platformě.
4. Porovnejte možnosti obou nasazených systémů z pohledu složitosti nastavení, poskytovaných služeb a možností konfigurace.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014, 622 s. ISBN 9788025138250.
2. PECINOVSKÝ, Josef a Rudolf PECINOVSKÝ. *Windows 10: průvodce uživatele*. Druhé, přepracované a aktualizované vydání. Praha: Grada Publishing, 2019, 268 s. Průvodce. ISBN 9788027124381.
3. HUNTER, Laura E. a Robbie ALLEN. *Active directory cookbook: solutions for administrators and developers*. 3rd ed. Sebastopol, CA: O'Reilly, c2009, xxv, 1059 s. ISBN 9780596521103.
4. STANEK, William R. *Active Directory: administrator's pocket consultant*. Redmond: Microsoft Press, c2009, xviii, 333 s. ISBN 9780735626485. Dostupné také z: http://www.loc.gov/catdir/enhancements/fy1006/2008940460-d.html
5. ALLEN, Robbie a Alistair G. LOWE-NORRIS. *Active Directory: implementace a správa Microsoft Active Directory*. Praha: Grada, 2005, 644 s. ISBN 8024709732.

Vedoucí diplomové práce: **Ing. Jiří Korbel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **2. prosince 2022**
Termín odevzdání diplomové práce: **1. června 2023**

L.S.

doc. Ing. Jiří Vojtěšek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 8. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne Bc. Patrícia Mravcová v.r

ABSTRAKT

Práca je zameraná na porovnanie doménových radičov na systémoch Linux a Windows. Bude sa jednať o inštaláciu a sprevádzkovanie oboch variant, porovnanie dostupných funkcií a nastavení, popis pripojenia zariadení (koncové stanice užívateľov, tlačiareň, atď.) do vytvorenej domény, popis správy užívateľov a ich prístupov k prostriedkom v doméne. Taktiež budú popísané možnosti zvýšenia bezpečnosti konfiguráciou bezpečnostných politík platných vo vytvorenej doméne.

Kľúčové slová: operačný systém, doménový radič, doména, koncový užívateľ, server

ABSTRACT

This diploma thesis is focused on comparing domain controllers based on Linux and Windows operating systems. It will be about installing and commissioning of both variants, comparing available functions and settings, describing the ways of connecting devices (end devices of users, printers, etc.) to the created domain, description of user management and their access to the resources in the domain. It will be also about the ways of increasing security by configuring security policies which are valid in the created domain.

Keywords: operating system, domain controller, domain, end user, server

Chcela by som sa poďakovať svojmu školiteľovi Ing. Jiřímu Korbelovi, PhD. za správne smerovanie a podporu pri písaní tejto diplomovej práce. Takisto by som sa chcela poďakovať mojim najbližším za podporu a momenty plných smiechu a radosti, aj keď to počas štúdia nebolo vždy jednoduché.

„Pro člověka, který chce a má vědomosti, není nic nemožné. “ – Tomáš Baťa

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Táto diplomová práca sa zaoberá konfiguráciou doménových radičov na systémoch Windows a Linux.

Doménový radič je server v počítačovej sieti, ktorý odpovedá na autentizačné požiadavky v počítačovej sieťovej doméne. Umožňuje prístup k prostriedkom domény pre počítače v doméne, ukladá informácie o užívateľských účtoch a vynucuje doménovú bezpečnostnú politiku.

Popísať v skratke, čo všetko doménový radič dokáže a nedokáže je takmer nemožné, škála funkcií je obrovská. Avšak jeho najdôležitejším aspektom je to, že sa dokáže integrovať s inými bezpečnostnými systémami (napríklad s dochádzkovým systémom, s informačnými systémami, účtovníckymi systémami, kamerovými systémami atď.) a takisto, že dokáže vo firemnej sieti (v doméne) korigovať prístup ku prostriedkom pomocou skupinových politík.

Táto diplomová práca je zameraná na prípravu doménových radičov tak, aby disponovali funkciami a rolami, ktoré sa najčastejšie konfigurujú.

Doménový radič je zariadenie, ktorého konfigurácia sa vždy „šije na mieru“ podľa potrieb – teda nie je dôležité, aby mal využitú celú funkcionalitu, ale aby plnil navrhnuté požiadavky. Jeho základ tvorí najmä databáza užívateľov, počítačov, skupín a organizačných jednotiek. Jeho cieľom teda je pripájať zariadenia a užívateľov do domény, kde na nich aplikuje nastavenia definované administrátorom a umožňuje zdieľanie a využívanie prostriedkov.

Doménové radiče založené na systéme Windows sú dnes bežnou záležitosťou každej firmy, zatiaľ čo doménové radiče na systéme Linux sú skôr experimentálne, ale ich funkcionalita sa vylepšuje a vyrovnáva systému Windows – momentálne ale v tejto chvíli má v tomto výhodu systém Windows.

I. TEORETICKÁ ČASŤ

1 TEÓRIA SIETÍ

Počítačová sieť sa dá charakterizovať ako skupina zariadení, ktoré sú vzájomne prepojené a môžu spolu komunikovať. Aby skupina zariadení mohla spolu v rámci počítačovej siete komunikovať, je potrebné, aby mali vo svojej výbave sieťovú kartu, ktorá im umožní komunikáciu, či už vo vnútornej sieti, alebo v rámci internetu. Internet je v podstate jeden mohutný komplex, kde spolu môžu komunikovať zariadenia po celom svete za dodržania určitých nárokov, podmienok a protokolov.

1.1 Adresovanie v počítačových sieťach

Aby bolo možné rozoznať, ktoré zariadenia chcú komunikovať a vymieňať si prostriedky, je potrebné ich identifikovať, v internete je to najčastejšie tromi spôsobmi:

- IP adresa
- Doménová adresa
- MAC adresa

1.1.1 IP adresa

IP adresa dostala názov podľa svojho protokolu, na ktorom beží a to anglicky Internet Protocol, známy hlavne vďaka svojej skratke IP. Tento prokotol vznikol v roku 1974 a je súčasťou tzv. rodiny protokolov TCP/IP. [1]

IP adresa jednoznačne identifikuje zariadenie v sieti, či už sa jedná o verejnú alebo privátnu sieť.

IP adresy sa v základe delia:

- Podľa rozsahu (triedy)
- Privátne, verejné (od providera)
- Podľa verzie použitého protokolu – IPv4, IPv6

Delenie podľa rozsahu (triedy):

- Na obrázku č.1 je delenie rozsahu privátnych IP adries.
- Na obrázku č.2 je delenie rozsahu verejných IP adries.

	Private address range	
Class	start address	finish address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Obrázok 1 : Delenie rozsahu privátnych IP adries. [2]

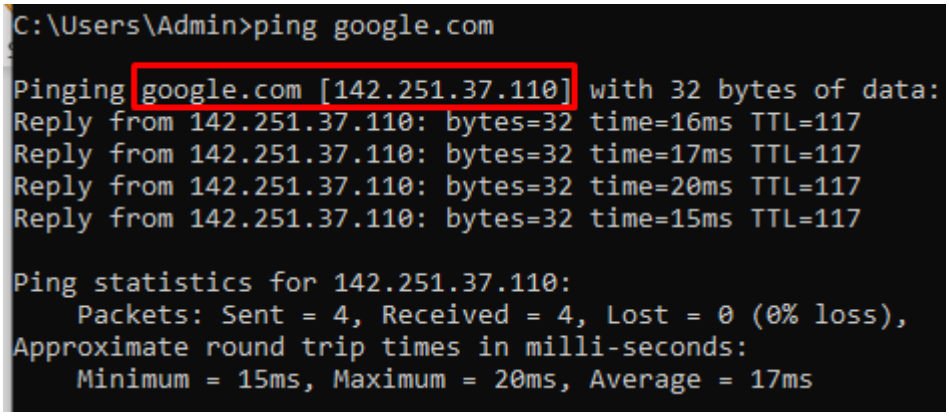
	Public address range	
Class	start address	finish address
A	0.0.0.0	126.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	254.255.255.255

Obrázok 2 : Delenie rozsahu verejných IP adries [2]

1.1.2 Doménová adresa

Doménové meno je v podstate preklad IP adresy na názov, ktorý je pre užívateľa jednoduchšie zapamätateľný, než samotná IP adresa. Tento preklad zabezpečuje protokol DNS (domain name system). Tento protokol zabezpečí pripojenie na IP adresu odpovedajúcu doménovému menu a užívateľovi zobrazí odpovedajúcu webovú stránku.

Na obrázku nižšie je vyvolaný v príkazovom riadku sieťový príkaz „ping google.com“, v červenom rámčeku je časť „google.com“ doménovou adresou, a časť „142.251.37.110“ je IP adresou serveru, kde tento web beží, teda DNS protokol preložil doménovú adresu na IP adresu.



Obrázok 3 : Príkaz ping v príkazovom riadku (vlastný zdroj)

1.1.3 MAC adresa

MAC (media access control) adresa je jedinečný identifikátor sieťového adaptéru – to znamená, že každý takýto sieťový adaptér by mal mať jedinečnú a nemennú MAC adresu. Je to tak z toho dôvodu, že na rovnakom segmente siete nesmú byť dva sieťové adaptéry s rovnakou MAC adresou. Avšak v praxi je všeobecne známe, že existuje napríklad MAC spoofing alebo iný software na falšovanie MAC adresy, takže MAC adresa nemusí, byť vždy jedinečná a nemenná.

1.2 Rozdelenie počítačových sietí

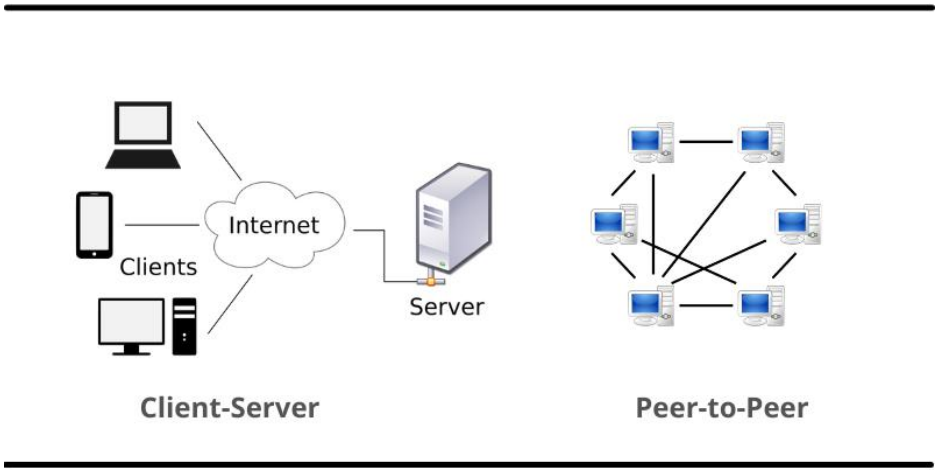
Počítačové siete je možné rozdeliť podľa mnoho kritérií, popísané budú tie najzákladnejšie kritériá delenia.

1.2.1 Rozdelenie pomocou použitého hardware

- Homogénne – zariadenia v sieti majú rovnakú hardware platformu
- Nehomogénne – zariadenia v sieti majú rôzne hardwarové platformy, operačné systémy, protokoly atp.

1.2.2 Rozdelenie podľa druhu pripojenia

- Peer-to-peer – komunikácia „rovný s rovným“, teda nie sú presne určené role zariadení (ktoré z nich je klient a ktoré z nich je server)
- Klient-server – sú to siete, kde majú zariadenia jasne definované svoje role (ktoré bude klient a ktoré bude server, ktorý bude spracovávať požiadavky klienta)



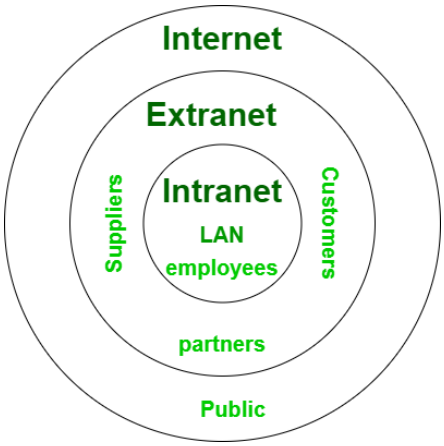
Obrázok 4 : Peer-to-peer vs. klient-server sieť [3]

1.2.3 Rozdelenie podľa spôsobov pripojenia

- Metalické pripojenie
- Optické pripojenie
- Bezdrôtové pripojenie (napríklad Wi-Fi)

1.2.4 Rozdelenie podľa účelu prevádzky siete

- Intranet – napríklad sieť vo vnútri organizácie, ktorá je využívaná zamestnancami. Táto sieť obsahuje väčšinou špecifické informácie a aplikácie dôležité pre každodennú komunikáciu vnútri organizácie.
- Extranet – je to predel medzi intranetom a internetom. Býva tak označená časť intranetu, ktorá je daná k dispozícii obchodným partnerom. Typickým príkladom extranetu sú systémy sledujúce stav objednávok a sledovanie požiadavkov obchodných partnerov. [1]



Obrázok 5 : Rozdiel medzi intranetom, extranetom a internetom [4]

1.3 Metóda SSO

Single Sign-on je metóda, kedy užívateľom stačí zadať svoje prihlasovacie údaje len raz a autentizácia (overovanie identity) k ďalším službám už prebieha bez zásahu. Tieto prihlasovacie údaje užívateľa sa nachádzajú na centrálnom mieste (serveri), na ktorom sa užívateľ autentizuje. SSO v podstate overí prihlasovacie údaje len raz a všetkým ostatným systémom / aplikáciám zaručí, že sú správne. Toto riešenie je vhodné najmä pre firmy, ktoré používajú viacero aplikácií, kedy by pre užívateľa bolo nevýhodné sa do každej aplikácie ktorú chce využívať musel prihlasovať opakovane.

SSO má svoje výhody a nevýhody. Medzi výhody patrí:

- Užívateľ sa nemusí autentizovať u všetkých služieb a aplikácií zvlášť
- Znižuje sa riziko prezradenia hesla
- Administrátor má pod kontrolou prístup do služieb a aplikácií na jednom mieste

Má však aj svoje nevýhody, medzi ktoré patrí:

- Autentizácia len pomocou jednych prihlasovacích údajov predstavuje riziko pri úniku, kedy bude mať útočník prístup k daným službám a aplikáciám
- Pokiaľ vypovedá službu centrálny server, na ktorom sa nachádzajú prihlasovacie údaje, užívateľ sa nikam neprihlási

Pre SSO existuje nespočet technológií, vzhľadom na praktickú časť diplomovej práce bude nasledujúca kapitola zameraná na Kerberos SSO.

1.3.1 Protokol Kerberos

Kerberos je sieťový autentizačný protokol, ktorý umoňuje komukoľvek komunikujúcemu v nezabezpečenej sieti bezpečne preukázať svoju identitu. Kerberos zabraňuje odposlúchavaniu a zaručuje integritu dát. Bol vytvorený primárne pre model klient-server a poskytuje vzájomnú autentizáciu – klient aj server si overujú identitu svojej protistrany. Kerberos je postavený na symetrickej kryptografii a preto potrebuje dôveryhodnú tretiu stranu. Štandardne používa port 88.

Kerberos je založený na Needham – Schroeder Symmetric Key Protocol. Používa dôveryhodnú tretiu stranu, ktorá sa nazýva Key Distribution Center (KDC), ktorá sa skladá z Autentizačného Serveru (AS) a Ticket – Granting Serveru (TGS). Kerberos pracuje na princípe tiketov slúžiacich k overeniu identity užívateľov.

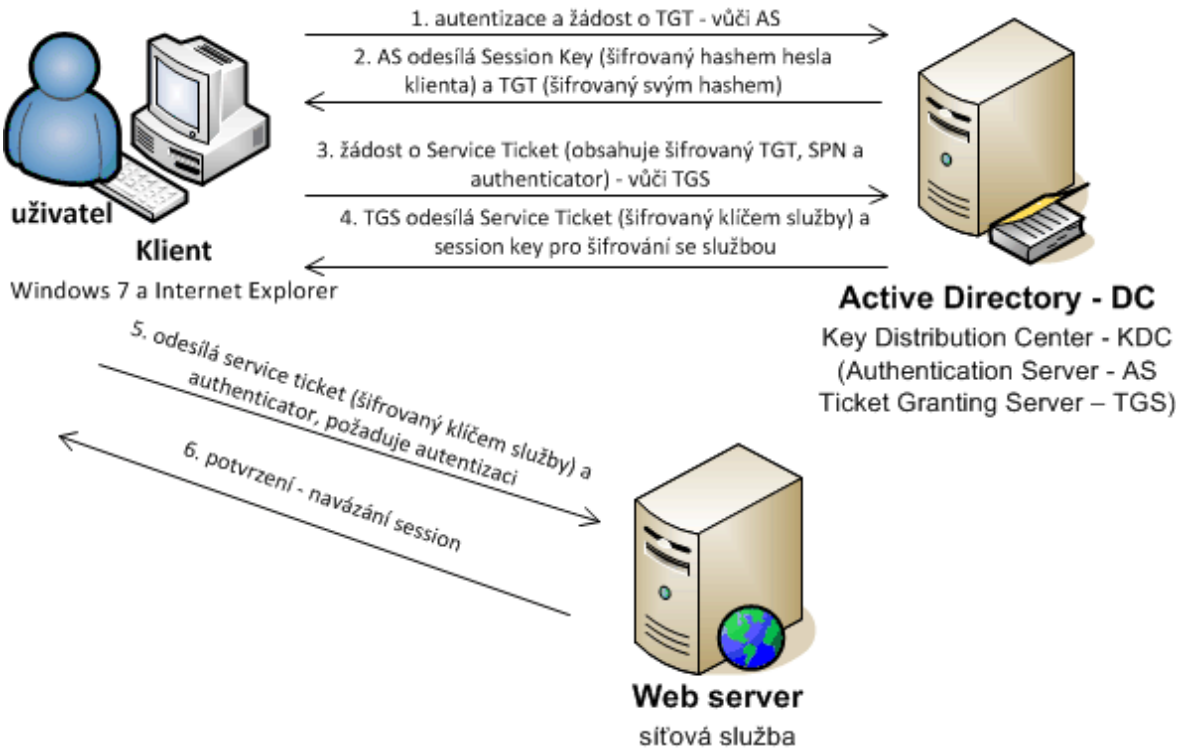
KDC si udržiava databázu tajných kľúčov – každá entita v sieti (či už je to klient alebo server) vlastní svoj tajný kľúč, ktorý je známy len KDC. Znalosť tohoto kľúča slúži k preukázaniu identity danej entity. Pre komunikáciu medzi entitami KDC vygeneruje „session key“, ktorým obe protistrany zabezpečia vzájomnú komunikáciu. Bezpečnosť tohoto protokolu významne závisí na vzájomnej synchronizácii času protistrán a krátkej životnosti tiketov.

1.3.2 Kerberos SSO

V tomto prípade realizuje autentizáciu služba KDC, ktorá beží na všetkých doménových radičoch. Klient teda musí mať pri využití SSO dostupný doménový radič (centrálne miesto, kde sa ukladajú prihlasovacie údaje). Túto službu nie je vhodné publikovať v internete, takže sa SSO obmedzuje na využitie vo vnútornej sieti. Na druhú stranu je však možné nastaviť dôveryhodnosť s inými doménami napríklad prostredníctvom VPN.

Služba, ku ktorej sa klient chce pripájať môže bežať na Windows serveri / stanici, ktorý môže, alebo aj nemusí byť zaradený do domény. Samozrejme tá služba môže bežať aj na iných systémových platformách (napríklad na Linux serveri).

Pokiaľ je užívateľ členom domény, tak si možno ani neuvedomuje, ako často dochádza k SSO. Hneď pri spustení počítača sa klient prihlasuje do domény zadaním prihlasovacích údajov, ktoré sa overujú voči doméne na doménovom radiči. Pokiaľ bude užívateľ využívať sieťovú tlačiareň, zdieľané disky, pripája sa Outlookom k Exchange serveri alebo iné sieťové služby, stále v pozadí bez jeho vedomia prebieha SSO. Keby tomu tak nebolo, musel by sa užívateľ samostatne ku všetkému prihlasovať ručne.[5]



Obrázok 6 : Princíp Kerberos SSO [6]

2 TEÓRIA OPERAČNÝCH SYSTÉMOV

Operačný systém sa radí medzi software vybavenie počítača, ktoré je zodpovedné za základné riadenie všetkých zdrojov počítača a komunikáciu s užívateľom. V podstate bez operačného systému nie je možné počítač používať (bola by možná komunikácia len na úrovni bitov 0 a 1), všetky príkazy sú operačným systémom prijímané a spracovávané a takisto programy využívajú pri svojej činnosti operačný systém.

V tejto časti sa budeme zaoberať výhradne operačnými systémami Windows a Linux, keďže v praktickej časti budú na týchto operačných systémoch bežať doménové radiče.

2.1 História operačných systémov

Na začiatku šesťdesiatych rokov operačné systémy ako také neexistovali. V šesťdesiatych rokoch sa objavujú prvé operačné systémy založené na disketách a diskoch – DOS pre IBM série 360. DOS bol dodávaný pre počítače firmy IBM, ktorá si ho nechala vyvinúť Microsoftom. Microsoft tento produkt nevyvinul sám, ale odkúpil licenciu na pôvodnú implementáciu zvanú QDOS (Quick-and-Dirty Operating System).

Pôvodný autor operačného systému, z ktorého vzišli všetky DOS-ovské verzie bol Tim Paterson. Keď v roku 1980 požadovalo IBM pre svoje 16 bitové počítače operačný systém, drobná začínajúca firma Microsoft sa podujala, že taký operačný systém naprogramuje. V skutočnosti však našla človeka, ktorý už mal operačný systém naprogramovaný, kúpila od neho práva a tie následne licencovala svojmu „tajnému“ klientovi IBM. Takto sa začala slávna éra Microsoftu.

Éra operačného systému Linux sa začína o kúsok neskôr. V roku 1990 sa fínsky študent Linus Torvalds skontaktoval s tvorcom Minixu (Unixu podobný OS), ktorého autorom bol Andy Tanenbaum, profesor počítačových technológií. Linus pôvodne plánoval vylepšiť Minix, ale Tanenbaum mu to nedovolil. Tak sa Linus rozhodol napísať svoje vlastné jadro, ktoré uvoľnil pod licenciou GPL v roku 1991. [7]

2.2 Funkcie operačného systému

Funkcie operačných systémov sa v podstate dajú rozdeliť na dve kategórie – jedna kategória definuje základné, integrované funkcie a druhá kategória hovorí o funkciách z užívateľského hľadiska, ktoré sa môžu v závislosti od daného typu operačného systému líšiť. Ďalej sa budeme teda zaoberať tými základnými (všeobecnými).

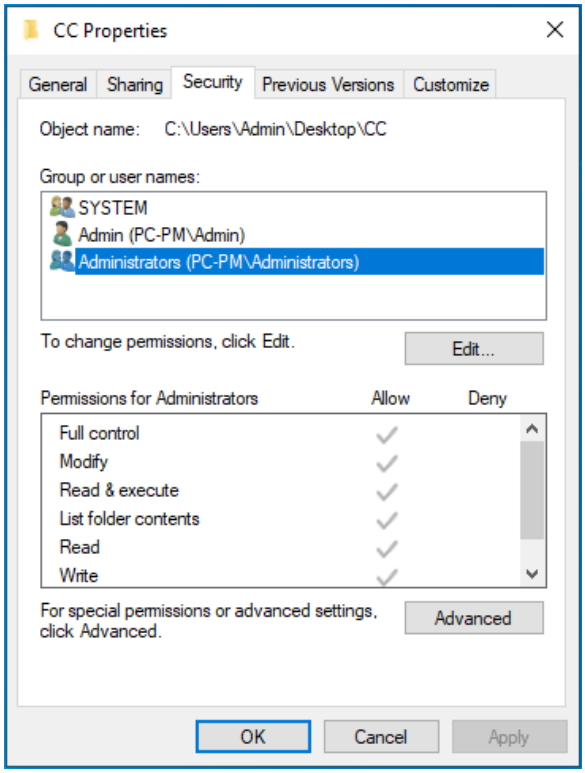
2.2.1 Správa súborov

Medzi primárne funkcie operačného systému patrí správa súborov a zložiek. To zahŕňa vytváranie, otváranie, zatváranie, aktualizácia a mazanie súborov / zložiek.

Operačný systém sa takisto stará o prístup k jednotlivým súborom, teda určuje, ktorý užívateľ má k akým súborom / zložkám prístup. Medzi oprávnenia k súborom a zložkám patrí čítanie, zápis, prezeranie zložky, plný prístup, čítanie + zápis, a špeciálne povolenia.

Funkcie OS pre správu súborov:

- Sleduje umiestnenie a stav súborov
- Prideľuje a odoberá zdroje
- Rozhoduje, ktorý zdroj má byť priradený ku ktorému súboru



Obrázok 7 : Ukážka povolení pre administrátorský účet pre zložku „CC“ (vlastný zdroj)

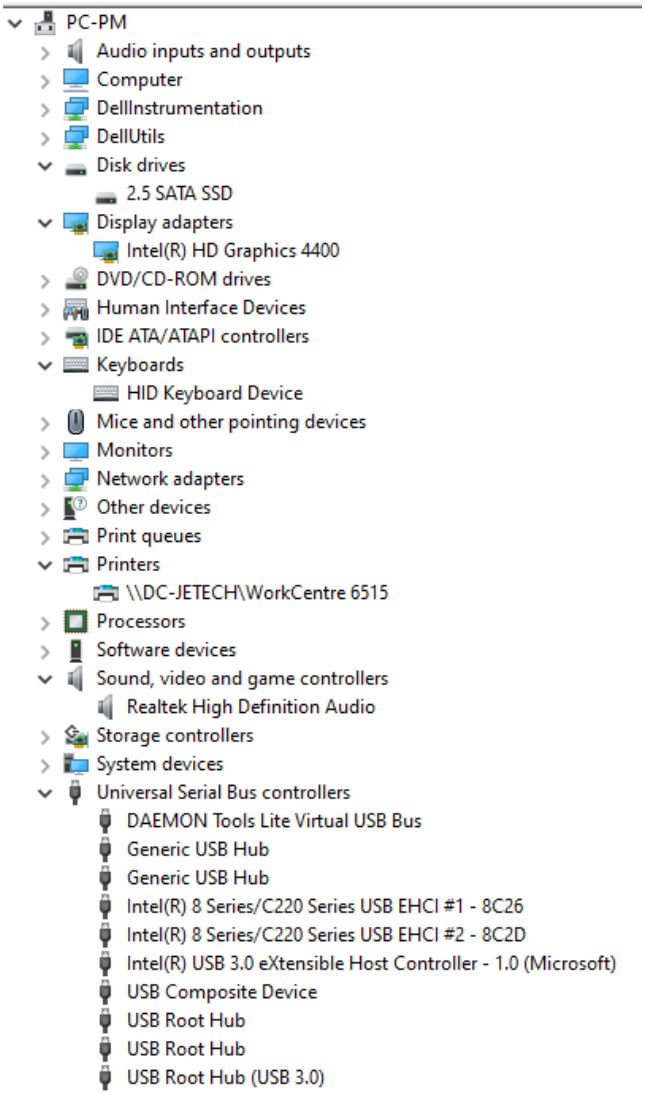
2.2.2 Správa zariadení

Operačné systémy poskytujú základné funkcie na správu zariadení pripojených k počítaču, medzi ktoré patrí: alokácia pamäte, spracovanie vstupných / výstupných požiadavkov a správa úložných zariadení. Medzi takéto zariadenia v podstate patrí čokoľvek, čo sa dá k počítaču pripojiť: tlačiareň, myš, klávesnica, rôzne karty do zberníc,

atp. V praxi to teda znamená, že OS komunikuje so všetkým, čo je pripojené k perifériám a zároveň aj s hardware na základnej doske pripojenom do zberníc (napríklad zvuková karta, grafická karta, atď.). Nutno dodať, že pripojené zariadenia potrebujú buď driver (špeciálny software, ktorý umožňuje OS komunikovať s hardware = typický scenár pre vnútorný hardware na doske), alebo periférie najčastejšie podporujú funkciu plug and play (čo v praxi znamená, že po pripojení napríklad myši do USB portu začne automaticky fungovať, nie je potrebné sťahovať dodatočný software, ani reštartovať počítač).

Funkcie OS pre správu zariadení:

- Prideľovanie / odoberanie zariadení rôznym procesom
- Uchovávanie záznamov o všetkých zariadeniach pripojených k počítači
- Rozhodovanie, ktoré zariadenie má byť pridelené ktorému procesu a na aký čas



Obrázok 8 : Ukážka pripojených zariadení v správcovi zariadení (vlastný zdroj)

2.2.3 Správa procesov

Medzi funkcie operačného systému patrí správa procesov, ktoré bežia na počítači. To zahŕňa spúšťanie a zastavovanie programov, prideľovanie prostriedkov a správu využitia pamäte. OS zabezpečuje, aby programy spustené na počítači boli kompatibilné a takisto je zodpovedný za presadzovanie zabezpečenia programu, čo pomáha chrániť počítač pred potenciálnymi útokmi.

Funkcie OS pre správu procesov:

- Prideľovanie / odoberanie zdrojov
- Prideľovanie zdrojov tak, aby sa systému nevyčerpali
- Ponúka mechanizmy na synchronizáciu procesov [8]

2.2.4 Správa pamäte

Jednou z najdôležitejších funkcií OS je správa pamäte. Ide o proces sledovania rôznych aplikácií a procesov spustených na počítači a všetkých údajov, ktoré používajú. Táto funkcia je veľmi užitočná najmä pre počítače s obmedzeným množstvom pamäte, pretože zaručuje, že žiadna aplikácia ani proces nezaberie príliš veľa miesta.

Keď sa počítač spustí, OS sa načíta do pamäte a potom spravuje všetky ostatné spustené programy. Kontroluje, koľko pamäte sa používa, koľko je k dispozícii a zabezpečuje, aby sa spustené programy vzájomne nerušili a neodoberali si potrebné zdroje.

Funkcie OS pre správu pamäte:

- Prideľovanie / odoberanie pamäte na ukladanie programov
- Rozhodovanie o množstve pamäte, ktorá má byť pridelená programom
- Distribúcia pamäte pri multiprocesingu
- Aktualizácia stavu v prípade uvoľnenia pamäte
- Uchovávanie záznamov o tom, koľko pamäte je využitej a koľko voľnej [8]

2.2.5 Správa zdrojov

Je to výkonný nástroj na sledovanie toho, ako sú využívané zdroje počítača – tieto informácie sú užitočné pri určovaní a riešení problémov s výkonom a pri identifikácii neoprávnených inštalácií software.

Funkcie OS pre správu zdrojov:

- Vedenie záznamov o všetkých aktivitách, ktoré prebiehajú v systéme
- Uchovávanie záznamov informácií o zdrojoch, pamäti, chybách atď.
- Sledovanie využitia pamäte
- Vytváranie systému súborov na organizáciu súborov a adresárov [8]

2.3 Dôležité pojmy viazané k operačným systémom

Multitasking, secure boot, multithreading, prerušenie, súborový systém, boot loader, POST

2.3.1 Multitasking

Multitasking je „zdanlivo“ súbežné spracovanie viacerých úloh počítačom. Prakticky funguje tak, že sa OS medzi jednotlivými programami / aplikáciami rýchlo prepína, pri čom vždy splní časť úlohy.

Moderné operačné systémy umožňujú „pravý“ multitasking tým, že spracovávajú úlohy paralelne (to sa netýka kooperatívneho a preemptívneho multitaskingu).

Typy multitaskingu:

- Kooperatívny multitasking – každá úloha je povinná dostatočne často systémovým volaním predať riadenie späť operačnému systému, vďaka čomu sa môže spustiť iná úloha a proces takto pokračuje pre všetky úlohy (delia sa o prostriedky). Podstatnou nevýhodou je, že pokiaľ bude úloha chybne naprogramovaná (teda nevráti riadenie späť operačnému systému), tak nastane úplné zastavenie systému aj ostatních úloh.
- Preemptívny multitasking – pri tomto type multitaskingu rozhoduje o prideľovaní a odoberaní prostriedkov úlohám samotný operačný systém. V pravidelných intervaloch s použitím časovača dochádza k prerušeniam aktuálneho procesu a následne sa vyhodnocuje situácia (ktoré úlohy žiadajú o prostriedky, ktorá úloha má vyššiu prioritu atď.) a buď OS prostriedky ponechá úlohe, alebo ich predá inej úlohe. Výhodou je, že pokiaľ by sa úloha zacyklila, tak jej OS prostriedky odoberie po uplynutí času. Nevýhodou je naopak zložitejšia implementácia a nutnosť hardware podpory v procesore.

2.3.2 Secure boot

Secure boot je metóda spúšťania operačného systému s overením, či sú všetky kľúčové súčasti operačného systému nezmenené a podpísané digitálnym podpisom. To prakticky znemožní spustenie upraveného operačného systému. [9]

2.3.3 Multithreading

Multithreading je schopnosť procesora, alebo jedného jadra v rámci viacjadrového procesoru vykonať viac procesov vhodne podporovaných operačným systémom. Multithreading teda umožňuje vykonávať viacero súbežných úloh v rámci jedného procesu.

2.3.4 Prerušenie

Prerušenie je funkcia operačného systému – je to signál, ktorý vyzve operačný systém, aby zastavil prácu na jednom procese a začal pracovať na ďalšom. Prerušenie môže byť buď zo strany hardware, alebo software a slúži na ukončenie procesu, ktorý sa správa tak, ako by nemal alebo reaguje neočakávane.

2.3.5 Súborový systém

Súborový systém zaisťuje ukladanie a čítanie dát pamäťového média tak, aby s nimi mohli užívatelia pracovať vo forme súborov a adresárov. Základnou ideou súborového systému je v podstate sprístupnenie a ukladanie dát pomocou hierarchicky organizovaného systému adresárov a súborov.

Súborový systém (file system) teda predstavuje:

- Spôsob organizácie dát na pevnom disku
- Dáta uložené v pomenovaných súboroch
- Hierarchickú štruktúru adresárov

Súborové systémy sú uložené na vhodnom type elektronickej pamäte, ktorá sa nachádza buď priamo v počítači (čiže HDD, SSD, prípadne CD atp.), alebo je to pamäť sprístupnená v počítačovej sieti. [10]

Existuje niekoľko typov súborových systémov, každý je svojimi parametrami charakteristický a súborové systémy pre operačné systémy Windows a Linux sa líšia (každý systém využíva iné typy).

Okrem typických súborových systémov pre operačné systémy existujú ešte špeciálne sieťové súborové systémy, napríklad SMB, NFC alebo CODA.

Súborové systémy používané operačným systémom Windows: FAT12 (zastaraný), FAT16 (zastaraný), FAT32, NTFS, exFAT, ReFS (využíva ho najnovší Windows 11)

Súborové systémy používané operačným systémom Linux: ext2 (zastaraný), ext3 (zastaraný), ext4, JFS, XFS, ReiserFS

Veľmi dôležitou súčasťou súborových systémov je žurnálovanie. Žurnálovanie je schopnosť súborového systému zapisovať každú operáciu s dátami do tzv. „žurnálu“ – čo zabraňuje strate údajov v prípade havárie. Funguje to tak, že po havárii sa jednotlivé operácie skontrolujú v žurnále (aby sa vytriedili na vykonané a nevykonané), nevykonané operácie akoby sa nestali. Nezabezpečuje to síce 100% ochranu pred stratou dát (dáta z nedokončených operácií sa stratia), ale významne sa znižuje ich počet. Za zmienku stojí, že z časového hľadiska sa žurnálujú len metadáta. [10]

2.3.6 Boot loader

Boot loader je zavádzač operačného systému, ktorého úlohou je načítať operačný systém do pamäte počítača pri štarte (obsahuje presné umiestnenie operačného systému na disku).

Existujú rôzne typy zavádzačov, pre Windows sú to MBR a GPT a pre Linux sú to GRUB, LILO, BURG (môže podporovať aj platformu Windows) a syslinux.

2.3.7 POST

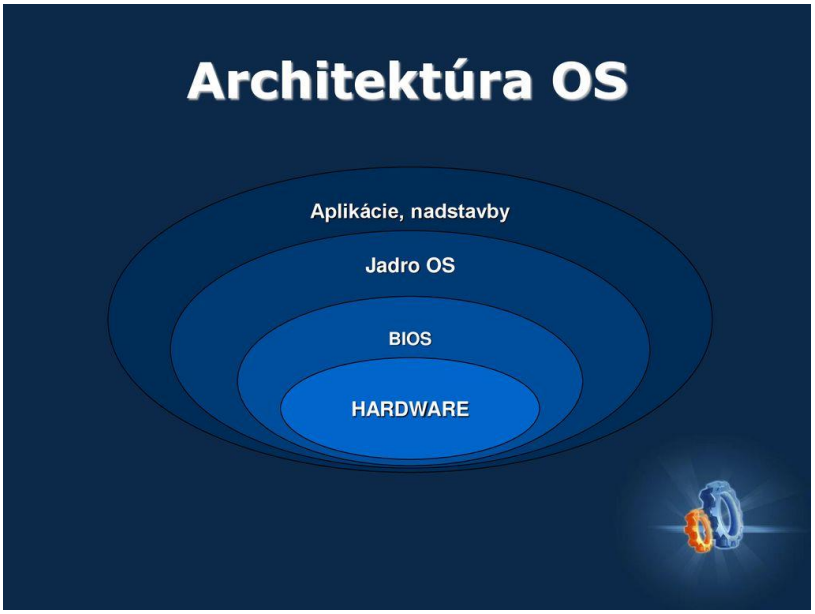
POST (power on self test) je proces, pri ktorom sa testujú a spúšťajú všetky komponenty PC. Najprv sa testujú komponenty, bez ktorých nemôže prebehnúť štart počítača (napríklad procesor, RAM atp. - pokiaľ budú poškodené, tak štart neprebehne) a následne sa testujú zvyšené komponenty, bez ktorých PC fungovať môže (napríklad zvuková karta).

2.4 Architektúra operačného systému

Operačný systém má spravidla hierarchickú (vrstvenú) architektúru, ktorá sa skladá z:

- Hardware
- BIOS a UEFI
- Jadro (kernel)

- Aplikácie, nadstavby [11]



Obrázok 9 : Schéma architektúry operačného systému [11]

2.4.1 Hardware

Hardware označuje všetko fyzicky existujúce vybavenie počítača - napríklad základná doska, zdroj, periférie, porty, procesor atď.

2.4.2 BIOS, UEFI

BIOS (basic input output system) je firmware pre osobné počítače. Používa sa najmä pri štarte počítača pre inicializáciu a konfiguráciu pripojených hardware zariadení a následnému spusteniu (zavedeniu) operačného systému, ktorému je potom predané ďalšie riadenie počítača. Programový kód BIOSu je uložený na základnej doske v nevolatilnej (stálej) pamäti.

UEFI je v podstate náhrada BIOSu, ktorá prišla spoločne s operačným systémom Windows 8. Tým došlo ku zmenám v pravidlách pre inštaláciu a zavádzanie operačných systémov.

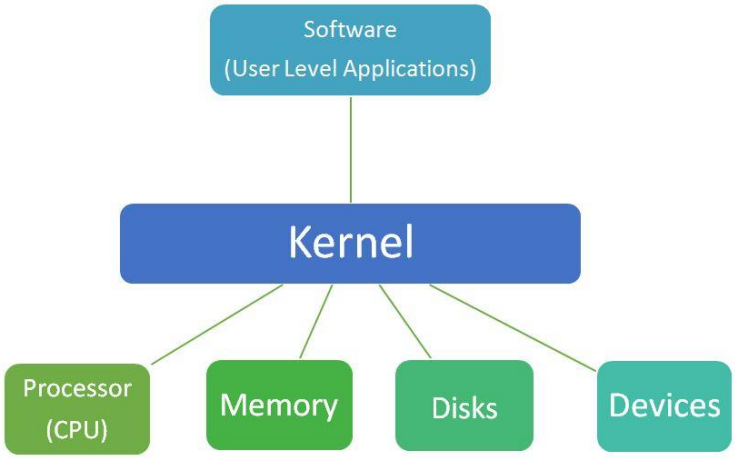
Rozdiely medzi BIOS a UEFI:

Tabuľka 1: Porovnanie BIOS a UEFI [12]

BIOS (legacy) boot mode	UEFI boot mode
Je tradičný a veľmi jednoduchý	Má lepšie grafické spracovanie
MBR formát pre diskové oddiely	GPT formát pre diskové oddiely
Bootovanie je pomalšie	Bootovanie je rýchlejšie
MBR formát pre diskové oddiely podporuje úložiská o maximálnej kapacite 2 TB	GPT formát pre diskové oddiely podporuje úložiská o maximálnej kapacite až 9 ZB
Beží v 16bit móde a podporuje navigáciu pomocou klávesnice	Beží v 32 až 64bit móde a poskytuje podporu pre navigáciu myšou a klávesnicou
Nepodporuje secure boot	Podporuje secure boot
Je komplexnejší oproti UEFI	Je jednoduchší na aktualizáciu

2.4.3 Kernel (jadro)

Časť operačného systému, ktorá je zodpovedná predovšetkým za správu a prideľovanie zdrojov (napríklad čas procesora, pamäť atp.) a správu periférií. Jeho základnými funkciami sú synchronizácia, medziprocesorová komunikácia, zasielanie správ a obsluha prerušení. Pre ostatné programy zaisťuje základné funkcie a veľmi často implementuje súborové systémy. [13]



Obrázok 10 : Kernel v operačnom systéme [14]

2.4.4 Aplikácie, nadstavby

Využívajú služby jadra. Medzi nadstavby OS patria:

- Interpreter riadiacich príkazov – načíta a interpretuje príkazy zadávané operačnému systému používateľom (napríklad z klávesnice)
- Externé príkazy – prechodné natiahnutie zodpovedajúceho kódu z disku
- Služobné programy
- Používateľské rozhranie – rozhranie, pomocou ktorého komunikuje operačný systém s používateľom (môže byť textové alebo grafické). [13]

2.5 Súčasti operačného systému

Medzi súčasti operačného systému patrí jadro, monitor a ovládače.

2.5.1 Jadro

Jadro je výkonná časť (exekutíva), ktorá je rezidentne umiestnená v pamäti. Podľa potreby sa inicializuje, alebo nahráva do pamäte ostatné dôležité časti operačného systému.

2.5.2 Monitor

Monitor je interpreter príkazov, ktorý zabezpečuje komunikáciu s užívateľom. Prijíma a analyzuje impulzy z klávesnice, zisťuje význam systémových príkazov a vypisuje príslušné odozvy na výstup.

2.5.3 Ovládače

Sú to obslužné programy vstupno – výstupných zariadení.

2.6 Všeobecné rozdelenie operačných systémov

Operačné systémy sa dajú rozdeliť podľa viacerých parametrov všeobecne, potom sa delia podľa počítačových platforiem (čo je popísané v kapitole 2.7).

2.6.1 Rozdelenie podľa použitia

- Nešpecializované – univerzálne, môžu prevádzkovať rôzne aplikácie
- Špecializované – pre úzko špecializovaný software (napríklad: databázové, vývojové, diagnostické …)

2.6.2 Rozdelenie podľa počtu užívateľov

- Monoužívateľské
- Viacužívateľské

2.6.3 Podľa počtu spracovávaných úloh a počtu procesov v systéme

- Jednoúlohové – súčasne môže byť spustená len jedna aplikácia
- Viacúlohové jednoprocesorové – súčasne môže byť spustené viacero aplikácií, ale úlohy sú prepínané v čase (nejedná sa teda o paralelný multitasking)
- Viacúlohové viacprocesorové – umožňujú paralelný multitasking

2.6.4 Rozdelenie z hľadiska podpory sieťových funkcií

- OS pre pracovné stanice – klientské počítače
- OS pre servery
- OS pre distribuované sieťové systémy (cluster, grid)

2.6.5 Rozdelenie podľa užívateľské rozhrania

- Textové užívateľské rozhranie (CLI) – k dispozícii je len príkazový riadok, do ktorého sa píšu príkazy, ktoré sú následne vykonané
- Grafické užívateľské rozhranie (GUI) – prívetivejšie k užívateľovi z hľadiska jednoduchosti a bez potreby znalosti príkazov (čiže obsahujú pracovnú plochu, kurzor, ikony …)

2.7 Rozdelenie operačných systémov na základe platformy

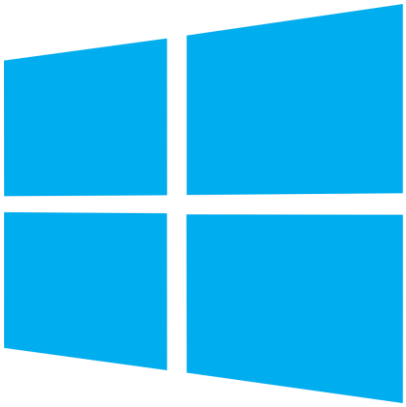
Platforiem pre osobné počítače existuje nespočetne, nasledujúce dve podkapitoly budú venované operačným systémom Windows a Linux, ktoré sú využité pre túto diplomovú prácu.

Zoznam ďalších známych platforiem: Mac OS, BSD, OS pre mobilné telefóny (napríklad iOS, Android), Solaris, AmigaOS atď.

2.7.1 Operačný systém Windows

Operačný systém Windows je najznámejší a najviac rozšírený operačný systém na celom svete (takisto to bol aj prvý operačný systém) a vyvíja ho firma Microsoft. Microsoft prvýkrát uviedol pod názvom Windows operačné prostredie v novembri 1985 ako nadstavbu

pre operačný systém MS-DOS (hlavnou motiváciou bolo grafické rozhranie, ktoré začalo, byť veľmi obľúbené). Operačné prostredia sa časom vyvíjali, Windows začal 16 bitovým operačným prostredím, nasledovali hybridy 16/32bitové operačné prostredia, až po aktuálne 64 bitové operačné prostredia. Aby to bolo upresnené, tieto operačné prostredia sa viažu na procesor, jednoducho povedané, 64 bitový procesor dokáže spracovať viac informácií naraz, uložiť viac výpočtov a celkovo je výkonnejší.



Obrázok 11 : Aktuálne logo operačného systému Windows [8]

Najviditeľnejší rys operačného systému Windows (od verzie 95 a NT 4.0) je tzv. pracovná plocha (desktop) a typické používateľské rozhranie (shell), ktoré sú podobné prostrediu „Workplace Shell“ uvedenom pre operačný systém OS/2 2.0 v roku 1992 od spoločnosti IBM, čo je objektovo – orientované grafické používateľské rozhranie (GUI) bežiace na OS/2 Presentation Manager. Rozhranie systému Windows však umožnilo obrovskú zmenu v spôsobe, akým ľudia a počítače navzájom komunikujú – grafické prostredie je jednoduchšie na ovládanie, zaniká nutná potreba znalosti príkazov, čo umožňuje aj menej skúseným užívateľom plné využitie vlastností a súčastí operačného systému. Súčasne ale nezanikol powershell a príkazový riadok, cez ktoré môže skúsenejší užívateľ zadávať príkazy a ovládať systém. [8]

Microsoft Windows vyvíja operačné systém pre osobné počítače, ale aj pre servery. Operačné systémy pre servery sú špeciálny druh operačného systému, ktorý je navrhnutý pre potreby sieťovej infraštruktúry (napríklad umožňuje konfiguráciu rôznych služieb, ako napríklad DNS, DHCP, Tlačový server, WSUS atď).

Takisto spoločnosť Microsoft ešte delí operačné systémy na rôzne edície a tými sú: Home, Pro, Enterprise (pre osobné počítače), Standard, Enterprise, Datacenter (pre servery) . Každá táto verzia má svoj účel:

- Edícia Home je určená pre bežného užívateľa, domácnosť, alebo mikrofirmu, neobsahuje žiadne špeciálne funkcie
- Edícia Pro je určená pre komerčných zákazníkov. Oproti edícii Home obsahuje naviac funkcie ochrany osobných údajov, funkcie zabezpečenia a funkcie správy
- Edícia Enterprise je určená pre organizácie s vysokým počtom užívateľov a je dostupná iba ako multilicencia
- Edície pre servery sa medzi sebou líšia obmedzeniami na množstvo virtuálnych systémov, podporovaného počtu jadier a dĺžky trvania licencie [15]

Aktuálna verzia OS Windows je Windows 11 a aktuálna verzia pre servery je Windows Server 2022. V praktickej časti diplomovej práce budú využívané systémy Windows Server 2022 pre doménový radič a Windows 10 Pro pre klientské počítače.

2.7.2 Operačný systém Linux

Ako už bolo zmienené v kapitole 2.1, Linux vznikol v roku 1990 a jeho autorom je Linus Torvalds.

V mnohých smeroch je Linux podobný konkurenčným operačným systémom, ako je napríklad Windows či macOS. Takisto ako konkurencia má grafické rozhranie, rovnaký typ software (kancelársky balíček, editor fotografií a podobne), je tam však jeden veľký zásadný rozdiel. Linux je tzv. „open - source“ projekt, čo znamená, že zdrojový kód je otvorený a každý si ho môže prispôsobiť podľa seba a takisto je dostupný úplne zdarma.

Jadro Linuxu je vo svojej podstate rovnaké, avšak sú distribuované rôzne jeho verzie – v praxi to znamená, že je Linux veľmi prispôsobiteľný, pretože nie je možné obmieňať len aplikácie, ale používatelia si môžu zvoliť aj základné komponenty, ktoré dávajú spolu „celok“. V súčasnosti medzi najznámejšie distribúcie patria napríklad Ubuntu, Fedora, SuSE, Mandriva, RedHat, Debian, Mint a ďalšie. Každá distribúcia sa v podstate hodí na iné použitie. Napríklad pre bežného užívateľa je vhodná distribúcia Ubuntu, zatiaľ čo napríklad pre servery sú vhodné napríklad distribúcie Debian a RedHat. [16]

Obrázok 12 : Logo Linuxu [17]

Linux disponuje textovým aj grafickým rozhraním, rozdiel oproti Windowsu je však v tom, že grafické rozhranie nepotrebuje pre svoje fungovanie, varianta bez grafického prostredia sa využíva pre serverové riešenia. (Príklady prostredí pre Ubuntu: Lubuntu, Xubuntu, Edubuntu atď.

Je faktom, že Linux sa skôr uchytil v serverových riešeniach, najčastejšie v podobe LAMP serverov (LAMP je skratka technológií Linux, Apache, MySQL a PHP). Dalo by sa povedať, že Linux využívajú dve kategórie ľudí:

- Sekretárka – keďže Linux je zdarma, pre firmy je veľmi výhodný, keďže nemusia kupovať licencie na systém a kancelárske balíčky
- IT professionál – hlavne teda webdesigneri, systémoví admini a programátori, ktorí si chcú systém škálovať a nemať v ňom zbytočne veľa súčastí, ktoré nevyužijú.

Čo sa týka využitia bežnými užívateľmi, Linux veľmi úspešný nie je, je to dané hlavne tým, že je proste "iný" ako Windows, využíva inú sadu aplikácií, častokrát nie je spätne kompatibilný s Windows aplikáciami (síce existujú emulátory, ale tie takisto vyžadujú znalosti, ktoré bežný užívateľ nemá) a celkovo bežný užívateľ častokrát nedokáže využiť jeho plný potenciál.

V rámci operačného systému Linux je ešte potrebné doplniť informácie, ktoré neboli uvedené v predošlých kapitolách – jedná sa však o doplnkové informácie. Teda inak povedané vo všeobecnej teórii sú všetky operačné systémy čo sa týka základných funkcií, architektúry, súčastí operačných systémov a dôležitých pojmov uvedených vyššie rovnaké (multitasking, secure boot, multithreading, prerušenia, súborový system, boot loader, POST…). Jediný rozdiel je v tom, aké technológie a spôsoby realizácie na to používajú.

Linux sa teda v základe líši iným grafickým prostredím (to je charakteristické pre každý OS), ale aj napríklad využívanými súborovými systémami, používa iné typy boot loaderov (napríklad GRUB alebo LILO), využíva iné shell príkazy, využíva vlastnú sadu programov, nevnucuje automatické aktualizácie atď.

3 TEÓRIA DOMÉNOVÝCH RADIČOV

V nasledujúcej kapitole bude zhrnutá teória týkajúca sa doménových radičov a jej súčastí vrátane praktického príkladu.

3.1 Praktický príklad využitia doménových radičov

Ako príklad možno použiť nasledujúcu situáciu. Podnikateľ s IT skúsenosťami bežného užívateľa založil firmu, kde na začiatok nakúpil pár zariadení – počítače, notebooky, tlačiareň a jednoduchý router na SIM kartu (plus samozrejme tarif od providera, aby v kancelárii mal prístup k internetu).

Všetky komponenty vybalil, uložil na stoly, kabelážou sa nemusel zaoberať, pretože má malú kanceláriu, kde bez problémov všade dosiahne signál Wi-Fi. Podľa návodu, ktorý našiel v krabičke od routra si ho ide nastaviť – pripojí sa k sieti, cez webový prehliadač sa prihlási cez default prihlasovacie údaje, zmení SSID (vysielaný názov siete) a heslo. Nič viac v podstate riešiť nemusí, sieť funguje, dnešné routre sú dimenzované na okamžité použitie bez nutnosti zložitejšej konfigurácie.

Zakúpi licencie na operačný systém, zvolí si tie najnovšie (z hľadiska stability a užívateľskej prístupnosti). Nainštaluje systém Windows 10 na zariadenia, pretože je v ňom zvyknutý pracovať a vytvorí lokálne účty pod menom Admin, ktorý má administrátorské oprávnenia.

Zistí, že k tlačiarni sa môže pripojiť len jeden zamestnanec prostredníctvom USB kábla – čo nie je pre neho ideálna situácia, pretože celkovo sú v kancelárii traja ľudia, ktorí budú potrebovať tlačiť. Problém vyrieši tak, že k tlačiarni pripojí počítač, z ktorého sa bude tlačiť. Týmto je infraštruktúra hotová a relatívne funkčná.

Postupom času sa firme začne dariť – získa nové zákazky, na ktorých popud musia byť expandované priestory firmy a nakúpené nové počítače. Zrazu už vo firme nie sú 3 zamestnanci aj s vedením, ale už je tam 15 zamestnancov v 5 rôznych kanceláriách. Tým pádom sa zvýšil počet zariadení, nároky na sieť a začali prichádzať problémy so zdieľaním tlačiarne a zároveň sa u zamestnancov s ich narastajúcim počtom objavujú rôzne problémy s ich zariadeniami (zamestnancom nefunguje internet, je nemožné dopátrať sa k vymazaným dokumentom, nastávajú bežné technické problémy – napríklad prestane fungovať nabíjačka na notebook, prestanú fungovať reproduktory atp.). Zároveň vedenie zistilo, že si zamestnanci musia medzi sebou predávať dokumenty prostredníctvom USB zariadení a

externých diskov, je v tom neporiadok, dokumenty sa začnú strácať, alebo si ich prezerajú neoprávnené osoby a situácia začína eskalovať. Doposiaľ funkčná infraštruktúra sa začína rozpadať a je potrebné hľadať vhodné riešenie týchto problémov.

Určite bude namieste zamestnať IT administrátora/IT technika, ktorý navrhne novú infraštruktúru, o ktorú sa bude starať, ďalej rozvíjať a riešiť technické problémy zamestnancov.

Návrh novej infraštruktúry:

Problematika:

Vo firme je momentálne 15 zamestnancov, ktorých počet občas stúpa, alebo klesá. Musia si medzi sebou „prehadzovať“ externé úložiská, ktoré majú tendenciu sa strácať, prípadne si ich občas zamestnanci privlastnia a vyberajú z nich informácie, ku ktorým nemajú mať prístup. Ten jeden pracovník, ktorého počítač je pripojený k tlačiarni už vlastne nie je administratívny pracovník, ale neustále musí riešiť kopírovanie, tlačenie a posielanie dokumentov. Rýchlosť internetu sa výrazne spomalila (s rýchlosťou 10 Mb/s pre 15+ zamestnancov sa dá takáto situácia očakávať), niektorým zamestnancom dochádza miesto na ich pevnom disku a nevedia si dať rady s bežnými technickými problémami.

Riešenie:

Riešenie sa ponúka vo vytvorení prostredia kde:

- Zamestnanci nebudú mať administrátorské oprávnenia (aby nemohli zariadenie prenastavovať a experimentovať s nastaveniami keď im niečo nefunguje)
- Zamestnanci budú mať možnosť zdieľať medzi sebou prostriedky bez nutnosti externých zariadení a keď im bude dochádzať miesto na pevnom disku ich zariadenia, budú mať možnosť si prostriedky ukladať na sieťový disk
- Bude tlačiareň dostupná pre všetkých bez nutnosti pripájania sa USB káblom
- Budú prostriedky uložené a rozdelené do skupín – aby sa k nim nikto, kto nemá oprávnenia nedostal
- Sa zvýši rýchlosť internetu atď.

Najprv je potrebné sa zakoncentrovať na nákup nových zariadení, ktoré sú potrebné pre vytvorenie novej infraštruktúry. Starý router sa z infraštruktúry odstráni a namiesto neho sa zakúpi menší rack, rackmount router, rackmount switch a dva počítače, ktoré budú slúžiť ako doménové radiče. IT administrátor alebo IT technik nakonfiguruje všetky zariadenia

podľa potreby (momentálne je dôležité vysvetliť dôležitosť doménových radičov v podnikoch, preto takýto postup konfigurácie nebude popísaný detailne).

Na počítač (server) sa nainštaluje serverovský operačný systém (napríklad Windows server 2022) a povýši sa konfiguráciou na úroveň doménového radiča. Na doménovom radiči sa postupne nakonfigurujú potrebné služby – DNS, DHCP, WSUS, tlačový server, BitLocker atp. Následne sa vytvoria na radiči vytvoria noví užívatelia, ich zariadenia sa pripoja do domény a zároveň prebehne konfigurácia bezpečnostných politík a radiče dostanú druhý disk (na ukladanie dát zamestnancov).

Doménové radiče musia byť vždy aspoň 2 (jeden primárny a jeden backup).

Čo sa zmenilo?

a) Užívatelia sa po novom prihlasujú prostredníctvom doménových účtov (tým pádom je napríklad na radiči vidieť ich aktivita) a nemajú práva administrátora, len práva, ktoré patria určitým skupinám (Príklad: skupina „programátori“ majú prístup do zložky projekty a zároveň sa vzdialene môžu pripájať k radiču, skupina „učtovnícky úsek“ má prístup do zložiek fakturácie, dane, výplatnice atď)

b) Radič disponuje dvomi diskami, na SSD beží operačný systém a HDD slúži ako extra úložisko pre zamestnancov a na odkladanie dát, ktoré sa majú zdieľať

c) Vďaka funkcii WSUS prebiehajú aktualizácie automaticky, bez nutnosti zásahu

d) Užívatelia nemajú neobmedzené administrátorské práva, takže nemôžu meniť nastavenia svojho zariadenia a komplikovať neodborným zásahom prácu IT administrátora

e) Po konfigurácii funkcie BitLocker sú disky v zariadeniach užívateľov šifrované, kľúč k odomknutiu ukladá radič

f) V prípade pádu systému je k dispozícii backup server

g) Tlačiareň je sieťová, má prístup k nej každý, radič disponuje uloženým driverom pre ňu, takže užívateľovi sa stačí len k nej pripojiť

h) A takto sa môže pokračovať ďalej podľa funkcií, ktoré sa podľa potrieb nastavia

Obrázok 13 : Prístup k zdrojom je podmienený autentifikáciou [18]

3.2 Role a funkcie Windows server

Role a funkcie Windows server sa inštalujú priamo na serveri, prostredníctvom Server Manager, ktorý je v podstate konzola pre správu. Vďaka tejto prehľadnej konzole si môže IT administrátor jednoducho inštalovať role a funkcie, prezrieť si ich stav a konfiguráciu.

Role a funkcie však nestačí len nainštalovať, vyžadujú ešte dodatočnú konfiguráciu podľa potreby.

Rola určuje primárny účel servera v sieti. Napríklad DHCP server rola pri správnej konfigurácii poskytuje klientom v sieti prideľovanie IP adries.

Funkcia rozširuje funkčnosť rolí, prípadne na nich môžu byť role závislé. [19]

Rolí a funkcií je naozaj veľmi veľký počet, preto v nasledujúcich podkapitolách budú podrobnejšie rozpísané len tie, ktoré priamo súvisia s touto diplomovou prácou.

3.2.1 Rola Active directory domain services (AD DS)

Služba AD DS predstavuje samotné srdce domén pre systémy Windows, konfiguruje sa priamo na doménovom radiči prostredníctvom povýšenia „obyčajného PC“ na vyššiu formu – teda doménový radič.

Je to veľmi intuitívna, flexibilná a bezproblémová implementácia autorizácie a autentifikácie pomocou protokolu Kerberos s podporou LDAP adresáru, ktorá je určená pre uloženie bezpečnostných, organizačných , aplikačných a konfiguračných dát pre užívateľov a počítače, ktoré sú replikované v georedundantnom prostredí odolnom voči chybám, ktoré je veľmi jednoduché na administráciu a pochopenie. [20]

3.2.2 Rola dynamic host configuration protocol server (DHCP)

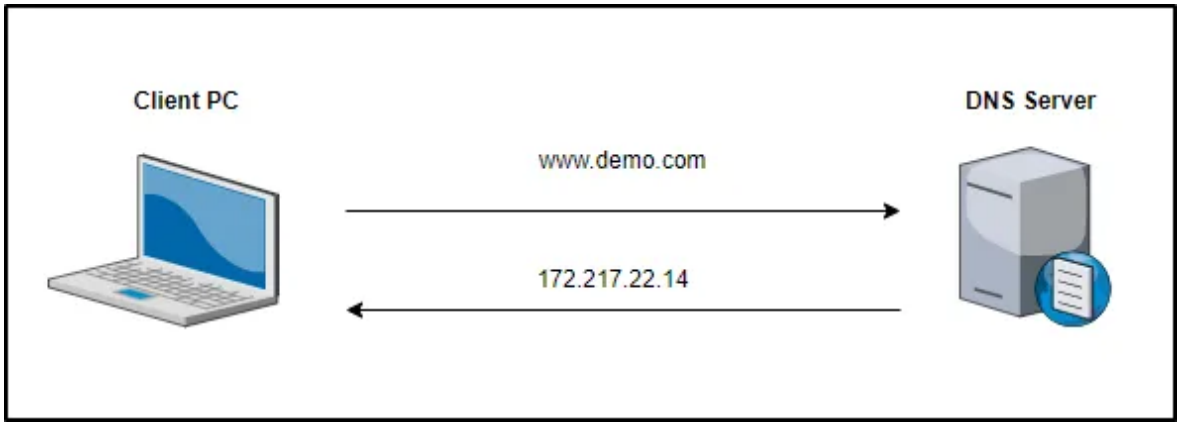
Táto rola plní funkciu prideľovania:

- IP adries staniciam na základe rozsahu alebo staticky
- Masiek na základe rozsahu
- IP adresy východzej brány
- IP adresy DNS serveru
- IP adresy WINS atp.

Na základe rozsahu sú myslené konkrétne rozsahy IP adries, ktoré sa v sieťach líšia, napríklad v praktickej časti tejto diplomovej práce sa pracuje s rozsahom 111.16.11.0/24.

3.2.3 Rola DNS (domain name server)

DNS poskytuje užívateľom jednoduchý spôsob komunikácie so zariadeniami na internete bez potreby pamätania si IP adries. V podstate sa jedná o preklad IP adresy na doménové meno (dopredný preklad), ale takisto je to aj naopak, len vtedy sa jedná o reverzný preklad.



Obrázok 14 : Schéma prekladu adries [21]

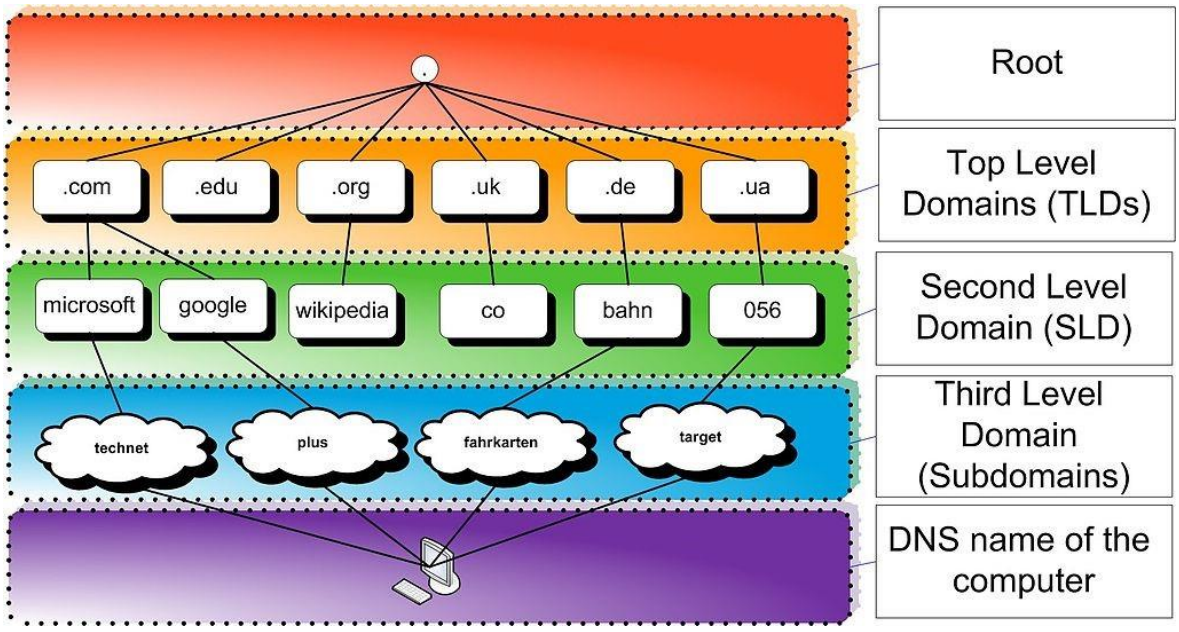
Komponenty DNS:

- Domain names – unikátne adresy na internete (najbližšie běžnému užívateľovi z hľadiska zapamätateľnosti), napríklad www.demo.com
- Name servery - servery pre ukladanie jednotlivých DNS záznamov pre domain names
- DNS records – slúžia pre základné nasmerovanie domény – teda určujú služby, ktoré sa budú na doméne využívať

Doménová hierarchia:

Všetky časti doménovej hierarchie sú zobrazené na obrázku nižšie pre lepšiu pochopiteľnosť.

- Root domain – najkratšia forma domény (tzv. „koreňová doména“). Táto doména je najvyššou úrovňou hierarchií internetu, ktorá prekonáva domény najvyššej úrovne (akými sú napríklad .com alebo .net atp.).
- Top-level domain – je to prípona, ktorá sa nachádza na konci názvu domény
- Second-level domain – druhá úroveň v doménovej hierarchii
- Subdomain – tretia úroveň v doménovej hierarchii



Obrázok 15 : Schéma hierarchie DNS s príkladmi [22]

DNS records (záznamy)

Ako bolo popísané vyššie, dns records slúžia pre základné nasmerovanie domény, existuje niekoľko typov:

- A record – obsahuje IPv4 adresu domény
- AAA record – obsahuje IPv6 adresu domény
- CNAME record – je alias, teda slúži k prideleniu viacerých doménových mien pre jednu IP adresu
- MX record – obsahujú adresy poštovných serverov pre doménu
- TXT record – slúžia pre uchovanie textového reťazca
- NS record - slúži pre určenie adresy, kde sú umiestnené DNS záznamy domény
- SOA record – je súčasťou každého zónového súboru, obsahuje informácie o platnosti DNS záznamu v sieti internet
- SRV record – udáva informácie o dostupnej službe a porte, na ktorom služba beží
- PTR record – reverzný záznam (presný opak A záznamu)

- Okrem vyššie uvedených záznamov existujú aj menej známe a používané, ktorými sú napríklad AFSDB, APL, CAA, CERT, DNAME atp. [21]

3.2.4 Rola file and storage services

Táto rola disponuje technológiami pre nastavenie a správu súborových serverov. Súborový server je server, ktorý umožňuje ukladanie súborov, ku ktorým majú sieťový prístup užívatelia (teda môžu na neho súbory ukladať, zdieľať, editovať, mazať atp.).

Táto rola je automaticky nainstalovaná, avšak bez pridaných funkcií. Pri inštalácii určitých rolí sa automaticky môžú nainštalovať aj ďalšie role, alebo funkcie. Odinštalovať sa samozrejme dá, ale len v špecifických prípadoch, v prípade povýšenia počítača na doménový radič zaniká možnosť túto službu FSS odinštalovať. [23]

3.2.5 Rola print services

Táto rola umožňuje nakonfigurovať na doménovom radiči print server. Pokiaľ je tlačiareň pripojená k print serveru tak má širšie možnosti konfigurácie (z hľadiska IT administrátora). Ako príklady budú uvedené tie najprínosnejšie výhody:

- Driver pre danú tlačiareň nemusí byť vyhľadávaný a inštalovaný ručne užívateľom (stačí ho dodať do databáze na drivery)
- Výborne funguje autentifikácia užívateľa prostredníctvom Kerberos-u

3.2.6 Rola web server

Web server používa protokoly (napríklad HTTP) na reagovanie na požiadavky klientov vykonané prostredníctvom WWW. Hlavnou úlohou web serveru je zobrazovať obsah webových stránok prostredníctom ukladania, spracovania a doručovania webových stránok užívateľom. Okrem HTTP protokolu podporujú web servery aj SMTP a FTP.

Hardware webového serveru je pripojený k internetu a umožňuje výmenu dát s inými pripojenými zariadeniami, zatiaľ čo software webového serveru riadi, jako užívateľ pristupuje k hostovaným súborom.

Táto rola priamo v diplomovej práci nefiguruje, je však potrebná pre fungovanie role WSUS. [24]

3.2.7 Rola windows deployment services

Táto rola slúži pre distribúciu pripravených obrazov operačných systémov. Umožňuje aj napríklad doplnenie ovládačov, nevýhodou je však to, že sa veľmi veľa vecí musí pripraviť manuálne, takže sa používa spolu s inými nástrojmi, ktoré túto činnosť odľahčujú.

3.2.8 Rola WSUS

Rola windows server update services slúži pre automatické aktualizácie software pre klientské stanice (teda nie sú potrebné manuálne aktualizácie pre každú klientsku stanicu zvlášť).

WSUS funguje tak, že si z oficiálnych serverov sťahuje aktualizácie (súčasti si môže administrátor navoliť podľa potrieb), ktoré sa následne distribuujú na klientské stanice za určitých pravidiel (ktoré nastaví administrátor).

Veľkou výhodou WSUS je to, že pokiaľ je nasadený spoločne s GPO, je možné na klientskej stanici nastaviť automatické aktualizácie tak, že ich nie je možné obísť alebo zrušiť užívateľom a tým porušovať interné pravidlá firmy a zároveň narúšať zabezpečenie celého systému.

3.2.9 Funkcie windows server

Ako bolo spomenuté vyššie, funkcie sú rozširujúcim doplnkom pre role, preto budú zhrnuté v tejto podkapitole.

Určité funkcie bývajú automaticky nainštalované tak, ako to býva u rolí. Niektoré funkcie a role sa inštalujú automaticky s inými rolami alebo funkciami.

S ohľadom na praktickú časť tejto diplomovej práce sem patria:

- .NET framework v aktuálnej verzii (prostredie pre beh aplikácií) – predinštalovaná funkcia
- Remote server administration tools (pre vzdialenú správu)
- Windows internal database – ukladajú sa v nej dáta týkajúce sa rolí a funkcií
- Windows powershell – predinštalovaná funkcia
- Microsoft defender antivirus – predinštalovaná funkcia pre základnú ochranu
- System data archiver – predinštalovaná funkcia pre archiváciu dát

- WoW64 support – preinštalovaná funkcia pre podporu behu 32-bit aplikácií na server core
- XPS viewer – predinštalovaná funkcia pre čítanie, nastavovanie oprávnení a digitálne podpisovanie XPS dokumentov
- Bitlocker drive encryption – slúži pre šifrovanie pevných diskov klientských staníc. Na odomknutie je potrebný recovery key, ktorý je uložený priamo v radiči a pre každé zariadenie je jedinečný
- Bitlocker network unlock – pokiaľ by nebola táto funkcia nainštalovaná, tak by sa po každom reštartovaní / vypnutí klienstkej stanice musel zádavať recovery key, čo je extrémne otravné a časovo náročné
- Enhanced storage – obsahuje bezpečnostné funkcie, ktoré umožňujú mať kontrolu nad tým, kto môže na zariadení pristupovať k dátam
- Group policy management- je to funkcia, ktorá sa automaticky inštaluje s rolou AD DS a slúži pre správu skupinových politík
- Windows server backup – umožňuje zálohovať a obnovovať OS
- Windows server migration tools – obsahuje nástroje pre migráciu systému

3.3 Skupiny zásad (group policy)

Skupiny zásad je nástroj pre hromadnú správu oprávnení a nastavení aplikovaných na počítač a užívateľa. V skupinách zásad je možné vytvárať kolekcie nastavení, ktorý sa nazýva Group Policy Object (GPO), ktoré dokážu meniť konkrétne parametre správania počítača alebo užívateľa. GPO sa potom ďalej „linkuje“ na jednotlivé organizačné jednotky (v organizačnej jednotke sa nachádzajú užívatelia, alebo počítače, na ktoré budú aplikované nastavenia).

Hlavné funkcie:

- Aplikovanie firemných štandardov (napríklad skrytie ovládacích panelov, sieťové tlačiarne, spúšťanie skriptov atp.)
- Aplikovanie zabezpečenia (napríklad parametre hesiel, zmena oprávnení prístupu k firemným zdrojom atp.)
- Hromadná inštalácia aplikácií (napríklad Office, aktualizácie, Adobe Reader atp.)

3.3.1 Politiky

Politiky sú v podstate samotné pravidlá, ktoré sa delia:

- Lokálne – lokálne politiky má každý počítač, aj ten, ktorý nie je pripojený do domény. Lokálna politika sa konfiguruje ručne na danom zariadení a platí len na ňom. Príkladom môže byť vytvorenie lokálneho užívateľa s obmedzenými právami (teda vytvorí sa užívateľský účet bez administrátorských oprávnení – bežný užívateľ)
- Doménové – tieto politiky platia len na zariadenia, ktoré sú pripojené do domény [25]

3.4 Komponenty active directory

Komponenty AD slúžia k formovaniu štruktúry adresára tak, aby odpovedala štruktúre organizácie a spĺňala jej potreby. AD má logickú a fyzickú štruktúru.

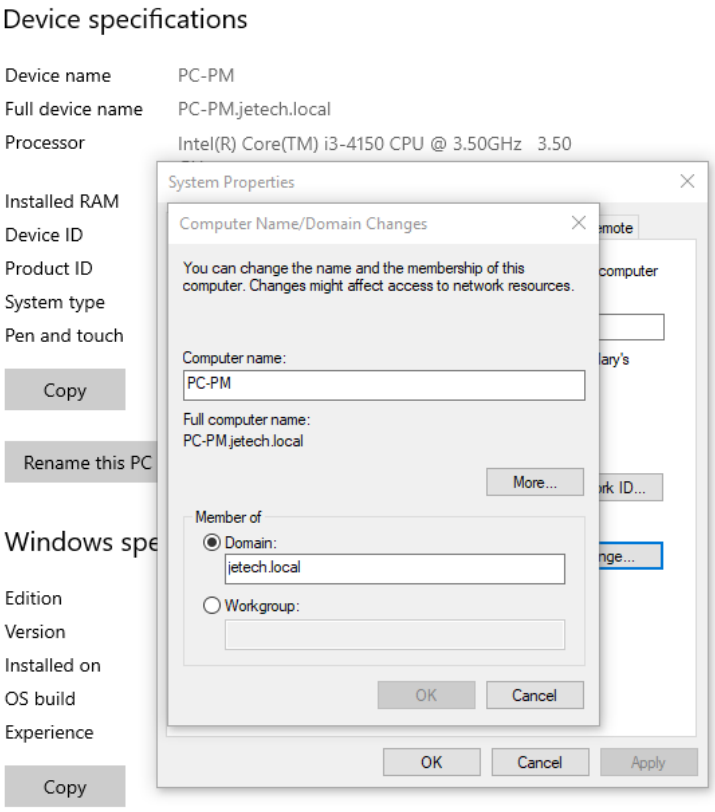
Logická štruktúra AD – je tvorená pomocou lesa, stromov, domén a OU. Na vrchole štruktúry bude bude vždy les – Forest. Les obsahuje stromy (trees) a samotný strom je tvorený jednou, alebo viacerými doménami. Vo vnútri domén sa nachádzajú jednotlivé organizačné jednotky (OU) a vo vnútri OU sa nachádzajú jednotlivé objekty (počítače, užívatelia, tlačiarne atp.)

Fyzická štruktúra AD – tá je tvorená pomocou doménových radičov a sites (sietí / podsietí). [26]

V nasledujúcich častiach si jednotlivé komponenty popíšeme.

3.4.1 Doména (domain)

Doména je základným prvkom logickej štruktúry AD. V doméne sú uložené objekty, ktoré do danej domény patria. AD môže byť tvorená jednou, ale aj viacerými doménami. Domény nie sú obmedzené na fyzické lokácie. [27]



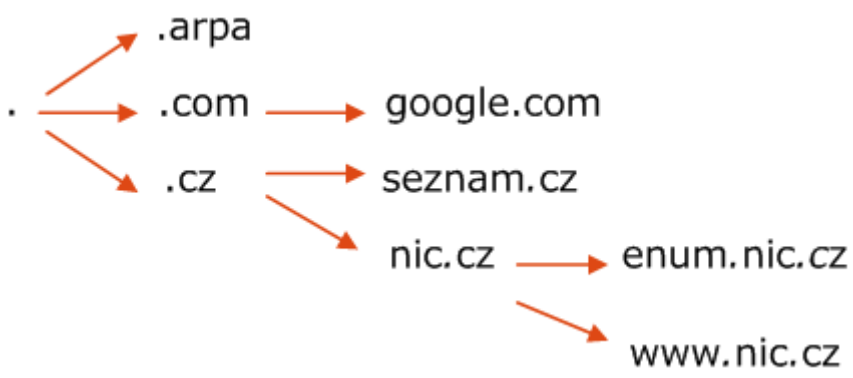
Obrázok 16 : Pripojenie zariadenia k doméne (vlastný zdroj)

3.4.2 Organizačná jednotka OU

V organizačnej jednotke sa nachádzajú objekty (to sú teda zariadenia, ktoré sa pripájajú k doméne – čiže počítače, notebooky, tlačiarne, NAS zariadenia atď.). Akýkoľvek objekt, ktorý chceme pripojiť do domény musí mať sieťovú kartu – teda musí disponovať IP adresou a schopnosťou komunikovať v rámci siete.

3.4.3 Strom (tree)

Strom môže byť tvorený jednou, alebo viacerými doménami. Vytvára sa pripojením podriadenej domény (child domain) ku koreňovej doméne (root domain). Používa sa DNS štandard, čo znamená, že doménové meno potomka (teda child domain) vznikne použitím jeho relatívneho mena za bodkou menom jeho rodičovskej domény (pre lepšie pochopenie viz. obrázok 13).



Obrázok 17 : Pomôcka k vysvetleniu DNS štandardu [28]

3.4.4 Les (forest)

Jeden alebo viacero stromov spoločne tvorí les. Les zdieľa spoločnú schému active directory a tá definuje AD databázu – čo v nej môže byť uložené a akú to má mať štruktúru.

V rámci lesa vždy existuje koreňová doména (forest root domain), jedná sa o prvú vytvorenú doménu v lese.

Všetky domény v rámci jedného lesa majú vytvorenú medzi sebou dôveru, tzv. „Two – way Transitive Trust“, teda obojsmerný vzťah dôvery, ktorý naviac nie je obmedzený len na dve priamo prepojené domény (šíri sa). Medzi koreňovými doménami stromov v rámci lesa sa vytvára dôvera – tzv. „Tree-Root Trust“ a medzi nadriadenými doménami sa vytvára tzv. „Parent Child Trust“. [26]

II. PRAKTICKÁ ČASŤ

4 ZÁKLADNÉ INFORMÁCIE A POSTUP

Praktická časť je zameraná na konfiguráciu doménových radičov, vybraných rolí (funkcií) a nastavenia skupinových politík. Po týchto krokoch nasleduje pripojenie zariadení k radičom a otestovanie funkčnosti nastavení.

Praktická časť prebieha priamo na fyzických zariadeniach, keďže nie je k dispozícii dostatočne výkonný hardware, na ktorom by bolo možné realizovať virtualizáciu (napríklad prostredníctvom VirtualBox, VMware atp.).

Všeobecne je odporúčané, aby mali doménové radiče minimálne jeden backup (čiže s konfiguráciou 1:1) z dôvodu možnosti znefunkčnenia pôvodného doménového radiča.

V praxi bývajú doménové radiče robustným systémom, ktorý sa ešte naviac môže integrovať s inými typmi domén (napríklad Microsoft 365) alebo inými systémami (napríklad so systémami kontroly vstupu, kamerovými systémami atp.). Teda takýto pád doménového radiča by spôsobil aj pád systémov (čiastočný alebo úplný), s ktorými je integrovaný a tým pádom by sa napríklad vážne mohla narušiť bezpečnosť firmy (vstupy, dáta, nedostupnosť prostriedkov atp.).

Doménový radič môže plniť veľmi veľa funkcií, má obrovskú škálu rolí, funkcií a možností konfigurácie – z toho dôvodu je nemožné nakonfigurovať kompletný doménový radič, vždy sa radič konfiguruje podľa aktuálnych požiadavkov a koniec koncov, role a funkcie sa môžu časom doinštalovať / dokonfigurovať podľa potrieb.

Takže na úvod praktickej časti je potrebné si definovať, na čo bude daný doménový radič slúžiť a aké role a funkcie bude využívať – týmto sa bude zaoberať nasledujúca podkapitola.

4.1 Požiadavky na doménový radič pre praktickú časť

Bude sa jednať o konfiguráciu doménového radiča pre firemné využitie (15 zamestnancov) s nasledujúcimi požiadavkami:

- Vytvorenie active directory s užívateľmi, zariadeniami a skupinami
- Vlastný DNS server pre preklad adries (z dôvodu bezpečnosti nie je vhodné vo firemnom prostredí používať DNS servery tretích strán)
- Prideľovanie IP adries pre všetky zariadenia v sieti
- Sieťová tlačiareň určená pre všetkých užívateľov v sieti

- BitLocker šifrovanie diskov pre zaistenie bezpečnosti firemných a osobných dokumentov
- Automatické aktualizácie operačných systémov všetkých zariadení bez nutnosti zásahu
- Nastavenie firemného úložiska pre užívateľov
- Nastavenie prístupu pre jednotlivých užívateľov / skupín na server a k firemným zdrojom

4.2 Príprava zariadení a sieťovej konfigurácie pre praktickú časť

Na to, aby mohla započať konfigurácia doménových radičov je potrebné si pripraviť spomínané fyzické zariadenia a testovaciu sieť. Na realizáciu praktickej časti budú použité zariadenia:

- 2x počítač pre doménové radiče a ľubovoľné testovacie zariadenia
- Router na SIM kartu pre vytvorenie testovacej siete
- Mini switch pre rozvetvenie portu routra (doménové radiče by mali byť pripojené kabelážou pre zabezpečenie stabilného pripojenia k internetu, vybraný router obsahuje len jeden port)
- Tlačiareň
- 4x UTP lankové káble s koncovkami RJ45

4.2.1 Počítače pre doménové radiče

Pre diplomovú prácu boli vybrané dva bazarové počítače značky DELL Optiplex 3020 s HW parametrami:

- Procesor: DualCore Intel Core i3-4160, 3600 Mhz
- Podpora rozlíšenia monitoru: 1920x1080 (FHD)
- Pamäť: 465 GB
- Sieťová karta: Realtek (R) PCI(e) Ethernet Controller MTU 1000
- RAM: 8 GB

Hardware bol overený z hľadiska dostatočnosti pre inštaláciu a chod operačných systémov server edícií Windows a Linux. Tieto informácie sa dajú overiť na oficiálnych stránkach vývojárov operačných systémov, kde sú uvedené minimálne hardware požiadavky, ktoré je ale potrebné vždy dimenzovať vyššie podľa potrieb.

4.2.2 Router na SIM kartu pre vytvorenie testovacej siete

Pre diplomovú prácu bol zakúpený bazarový router STRONG 4G LTE. Tento router disponuje:

- 2x slot pre SIM kartu ľubovoľného operátora
- 2x 4G LTE anténa
- Maximálnou rýchlosťou Wi-Fi 300 Mbit/s
- 1x ethernetový port

V podstate nie je potrebný žiaden výkonný router s podporou vysokých prenosových rýchlostí.

4.2.3 Mini switch pre rozvetvenie portu routra

Pre diplomovú prácu bol zakúpený bazarový mini switch značky tp-link. Tento switch disponuje:

- 5x ethernet port 10/100 Mbit/s
- Maximálnou rýchlosťou 200 Mbit/s
- Funkciou Plug and Play

4.2.4 Tlačiareň

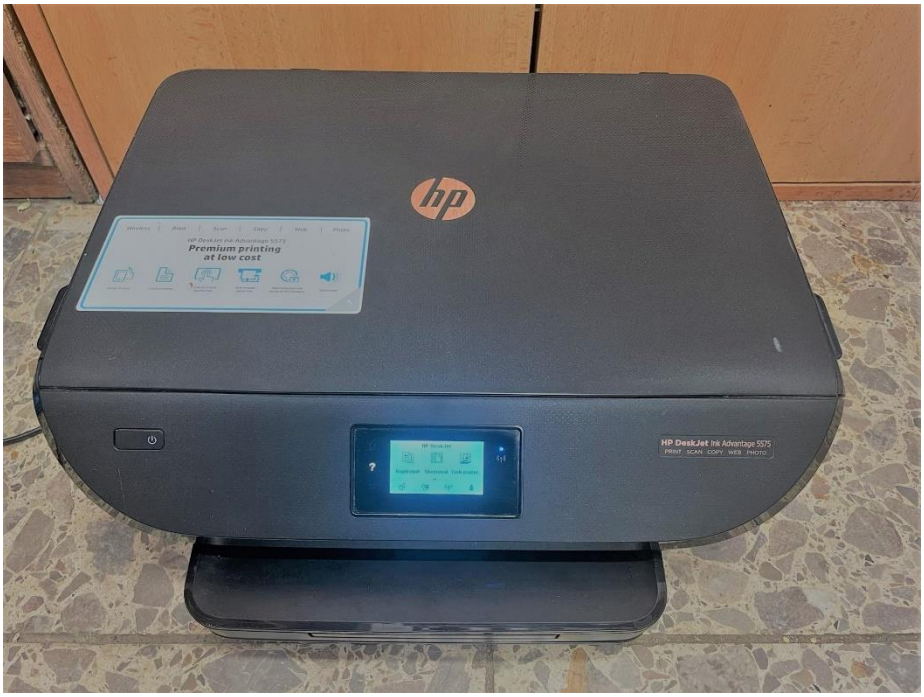
Pre túto diplomovú prácu bola vybraná sieťová tlačiareň HP DeskJet Ink Advantage 5575. Táto tlačiareň disponuje:

- Funkciami tlačiarne, skeneru a kopírky
- Obojstranným tlačením
- Dotykovým displejom

4.2.5 UTP lankové káble s koncovkami RJ45

Pre diplomovú prácu boli zakúpené 2x UTP lankové káble s koncovkami RJ45. Netienená kabeláž pre praktickú časť stačí, hardware sa nebude nachádzať v prostredí, kde by hrozilo rušenie.

Obrázok 18 : Pripravené zariadenia pre praktickú časť 1 (vlastný zdroj)



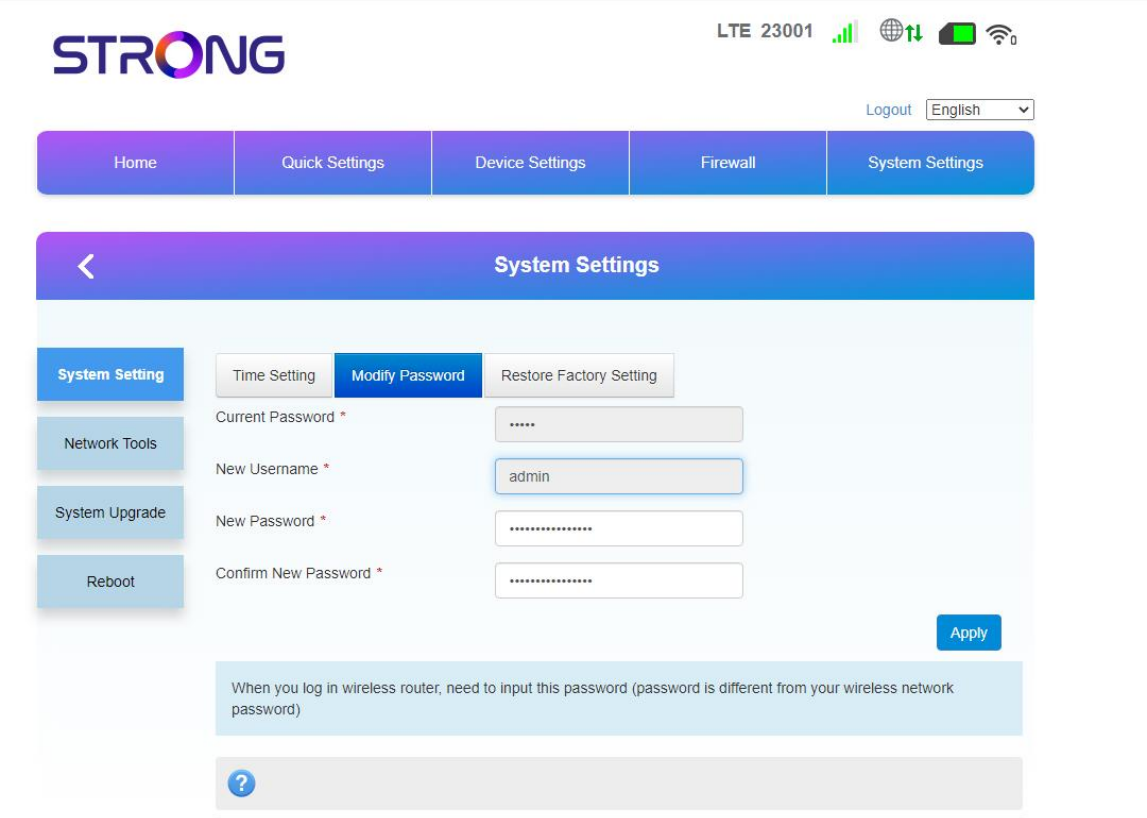
Obrázok 19 : Pripravené zariadenia pre praktickú časť 2 (vlastný zdroj)

4.2.6 Príprava sieťovej konfigurácie

Doménové radiče sú zariadenia, ktoré bez siete nemôžu fungovať. Na začiatok je potrebné si pripraviť testovaciu sieť. Postup je jednoduchý – dnešné štandardné routre majú veľmi jednoduchý postup konfigurácie z užívateľského hľadiska. Okrem nastavenia základných informácií bude potrebné nastaviť sieťový rozsah adries (zatiaľ ešte nie sú nakonfigurované doménové radiče, ktoré by spĺňali rolu DHCP servera, takže zatiaľ túto rolu preberie router). Pre túto diplomovú prácu bol vybraný rozsah 111.16.11.0/24.

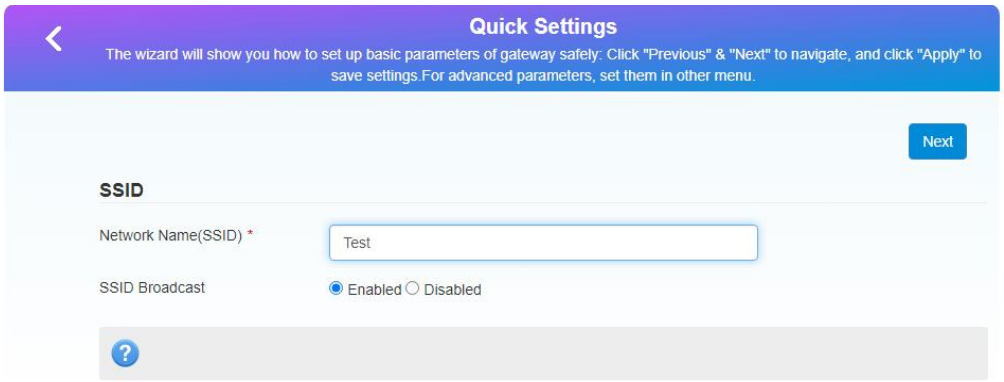
Pre konfiguráciu routra je najprv potrebné dostať sa do jeho webového rozhrania, štandardne stačí router prepojiť krútenou dvojlinkou s počítačom a pristúpiť do jeho webového rozhrania prostredníctvom webového prehliadača, kde je potrebné zadať jeho default IP adresu a prihlasovacie údaje (najčastejšie to býva IP adresa 192.168.1.1 s prihlasovacími údajmi admin / admin).

Vždy po prihlásení je potrebné zmeniť default prihlasovacie údaje na vlastné, inak by router predstavoval bezpečnostnú hrozbu.

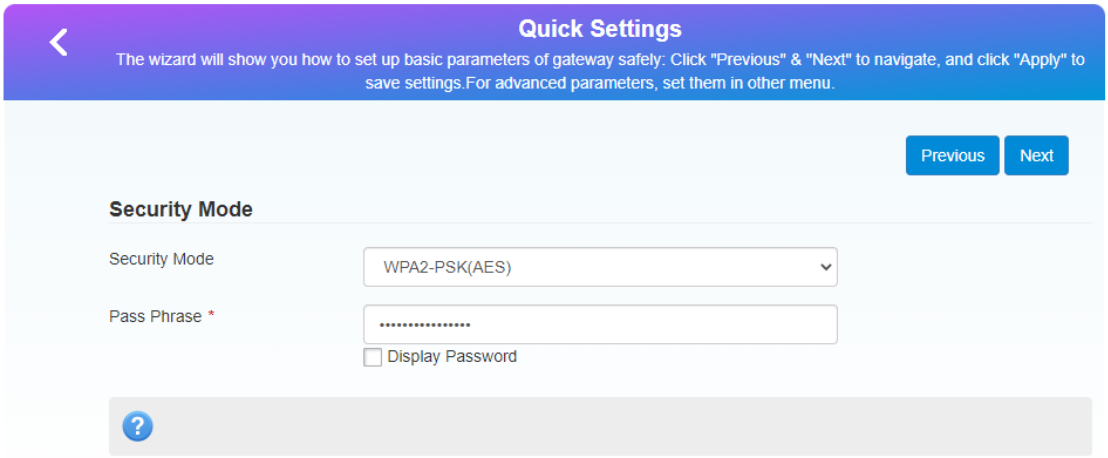


Obrázok 20 : Zmena prihlasovacích údajov (vlastný zdroj)

Pod záložkou „Quick Settings“ sa nachádza sprievodca základnou konfiguráciou, kde je nastavené SSID siete „Test“, heslo k pripojeniu a režim šifrovania.



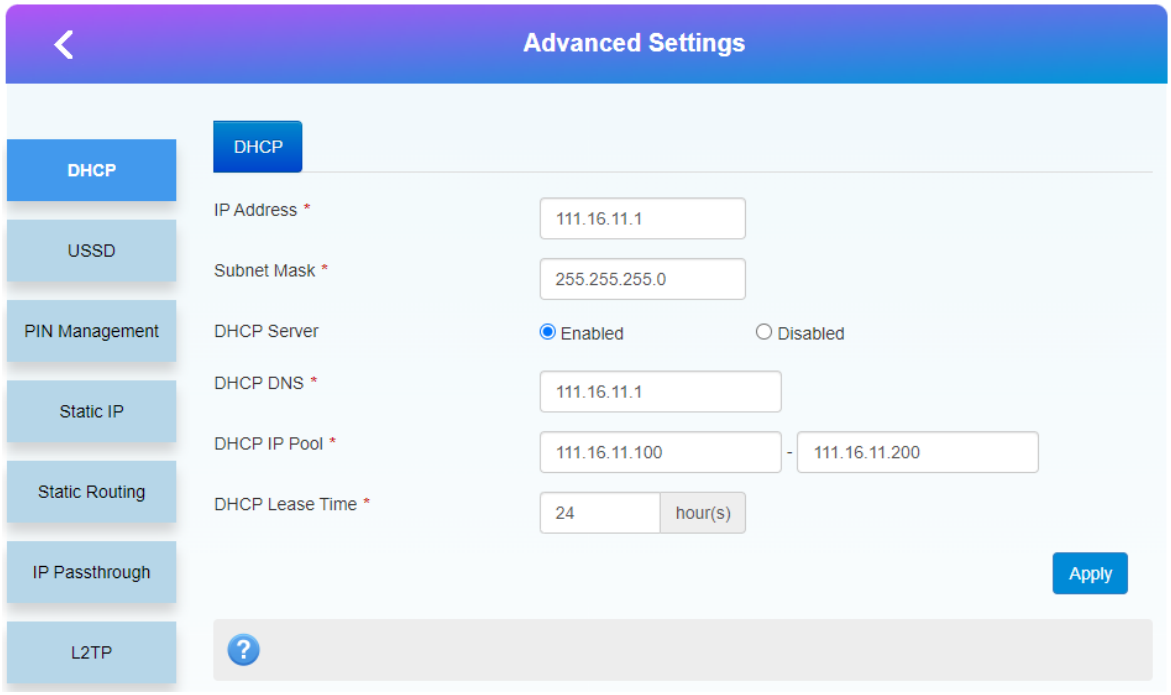
Obrázok 21 : Nastavenie SSID siete (vlastný zdroj)



Obrázok 22 : Nastavenie režimu šifrovania a hesla

Teraz bude potrebné nastaviť službu DHCP s vybraným rozsahom 111.16.11.0/24. Neskôr túto funkciu preberie doménový radič. Rozsah prideľovania pre zariadenia bol nastavený od 111.16.11.100 do 111.16.11.200. Doménový radič, ktorý sa bude pripájať do siete môže mať na obmedzenú dobu pridelenú adresu pomocou DHCP (kým sa urobia potrebné nastavenia).

Po tomto kroku je potrebná konfigurácia dokončená, ešte sa podľa potrieb však neskôr bude meniť.



Obrázok 23 : Nastavenie služby DHCP (vlastný zdroj)

5 PRÍPRAVA DOMÉNOVÉHO RADIČA – SYSTÉM WINDOWS

Ako prvým sa začne príprava doménového radiča systému Windows. Tento doménový radič bude disponovať grafickým prostredím (na rozdiel od Linux, ale o tom neskôr v inej kapitole). V nasledujúcich kapitolách budú rozpísané kroky, ktoré sú potrebné pre prípravu Windows DC s požiadavkami, ktoré boli uvedené v kapitole 5.1. Cieľom tejto kapitoly nie je poskytnúť komplexný návod na konfiguráciu doménového radiča.

Ešte je nutné poznamenať, že pri jednotlivých konfiguráciách nie sú vložené všetky obrázky jednotlivých krokov – nejedná sa však o dôležité kroky, naopak, jedná sa o okná s informáciami, ktoré nie sú potrebné dokumentovať.

5.1 Inštalácia operačného systému Windows Server 2022

Prvým krokom je samozrejme nainštalovať samotný operačný systém.

5.1.1 Stiahnutie operačného systému

Microsoft svoje operačné systémy umožňuje sťahovať zdarma s tým, že sú aktívne len po určitú dobu, následne je potrebné ich licencovať (čiže zakúpiť si licenciu na oficiálnych stránkach a zadať product key).

V tejto práci nebude využitá možnosť stiahnutia operačného systému Windows za podmienky aktivácie, pretože samotný Microsoft poskytuje licencie na testovanie pre študentov zdarma.

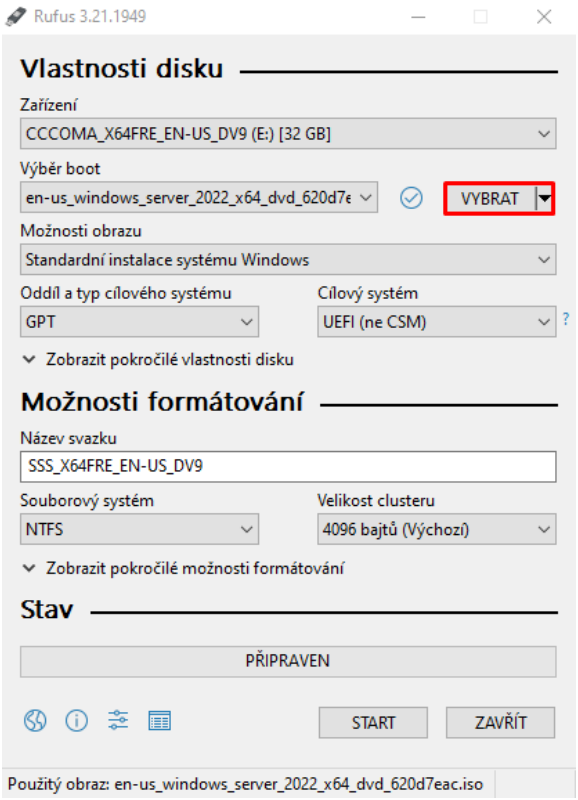
Stačí si daný SW stiahnuť z oficiálnych Microsoft stránok pre edukáciu (education hub), kde je zároveň poskytnutý product key. Na stiahnutie daného SW je však potrebná registrácia, kedy si Microsoft prostredníctvom e-mailu overuje, či sa naozaj jedná o študenta (tenantom musí byť školské zariadenie).

5.1.2 Príprava inštalačného média

Na prípravu inštalačného média je najvhodnejšie použiť SW tretej strany – najčastejšie používaným je buď windows creation tool, alebo napríklad Rufus.

V tejto práci bude inštalačné médium pripravené prostredníctvom SW Rufus.

Rufusa si stačí stiahnuť z oficiálnych stránok, existuje aj portable verzia.



Obrázok 24 : Príprava inštalačného USB (vlastný zdroj)

V podstate nie je potrebné nič z preddefinovaných parametrov meniť, stačí len vybrať ISO súbor zo zoznamu a kliknúť na „start“.

Keď Rufus dokončí prípravu inštalačného média, stačí ho zavrieť a týmto je inštalačné médium pripravené na použitie.

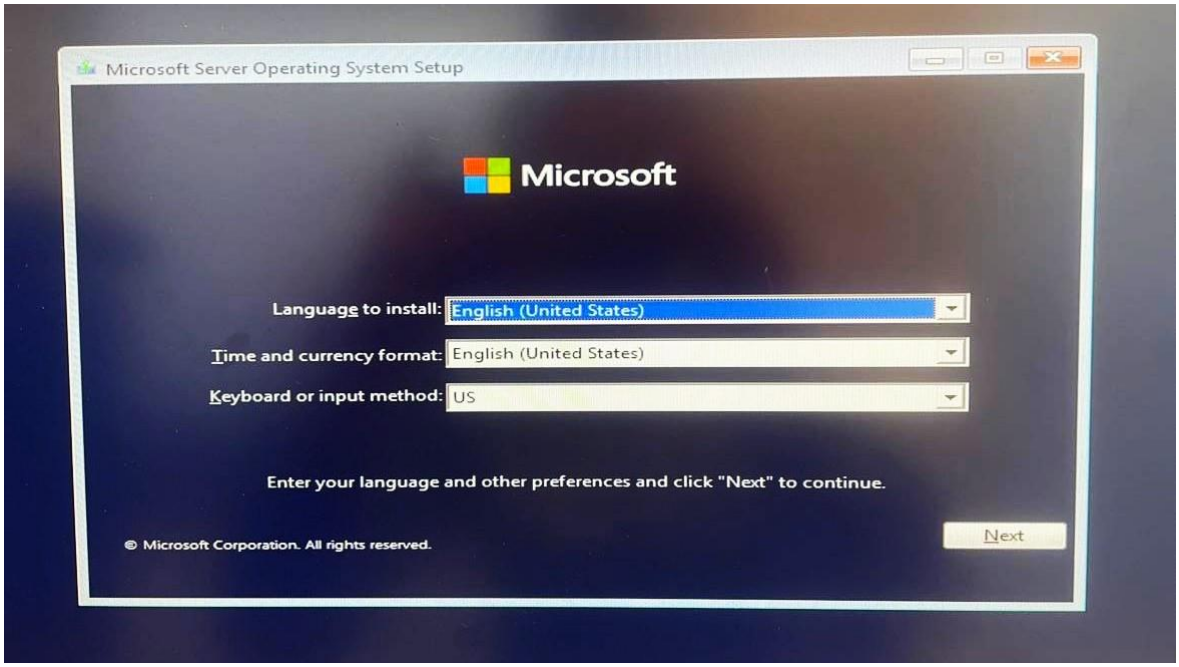
5.1.3 Samotná inštalácia operačného systému

Na samotnej inštalácii operačného systému nie je nič komplikovaného, azda len vybranie vhodného hesla pre „Administrator“ lokálny účet. Lokálny účet je dôležitý, a je dôležité si k nemu pamätať prihlasovacie údaje, pretože doménový účet nemusí byť vždy dostupný.

Začne sa tým, že je potrebné sa premiestniť do BIOSu alebo UEFI. To sa realizuje stlačením určitých tlačidiel pri štarte počítača. V prípade vybraného modelu je to tlačidlo „Delete“.

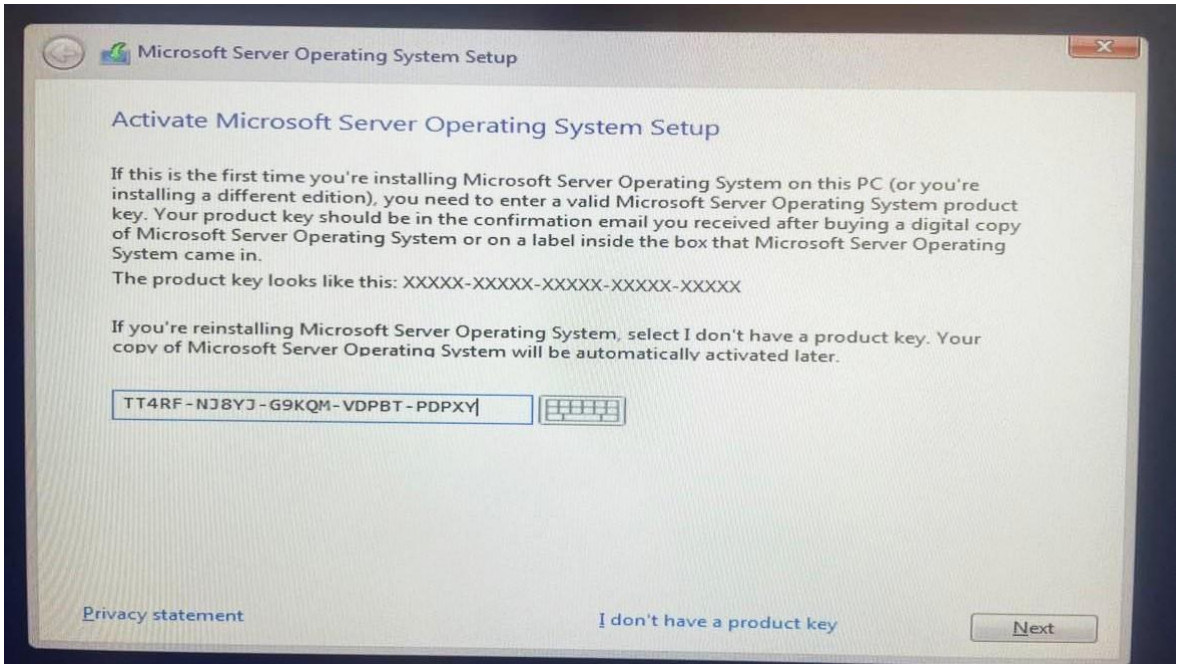
Po úspešnom premiestnení bolo potrebné nastaviť poradie bootovania tak, aby bootovanie z USB kľúča bolo na prvej pozícii a zároveň boli ostatné metódy zakázané. Nie je totiž potrebné bootovať pôvodný operačný systém, ale naopak začať inštalovať nový.¨

Ďalším krokom je výber jazyka – vybraný bol anglický jazyk.



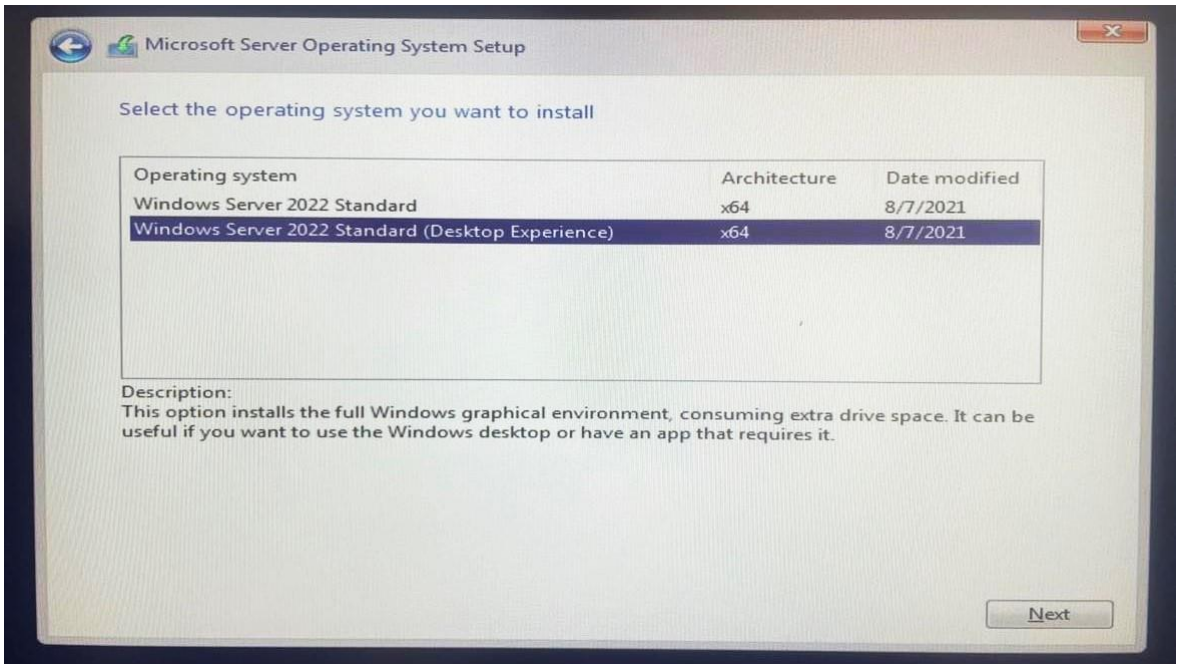
Obrázok 25 : Výber jazyka pre systém windows (vlastný zdroj)

Ďalší krok inštalácie spočíva v možnosti zadať product key, túto možnosť ide samozrejme preskočiť a zadať ho neskôr. Tu bude použitý product key, ktorý vygeneroval Microsoft pre testovacie účely k účtu p_mravcova@utb.cz.



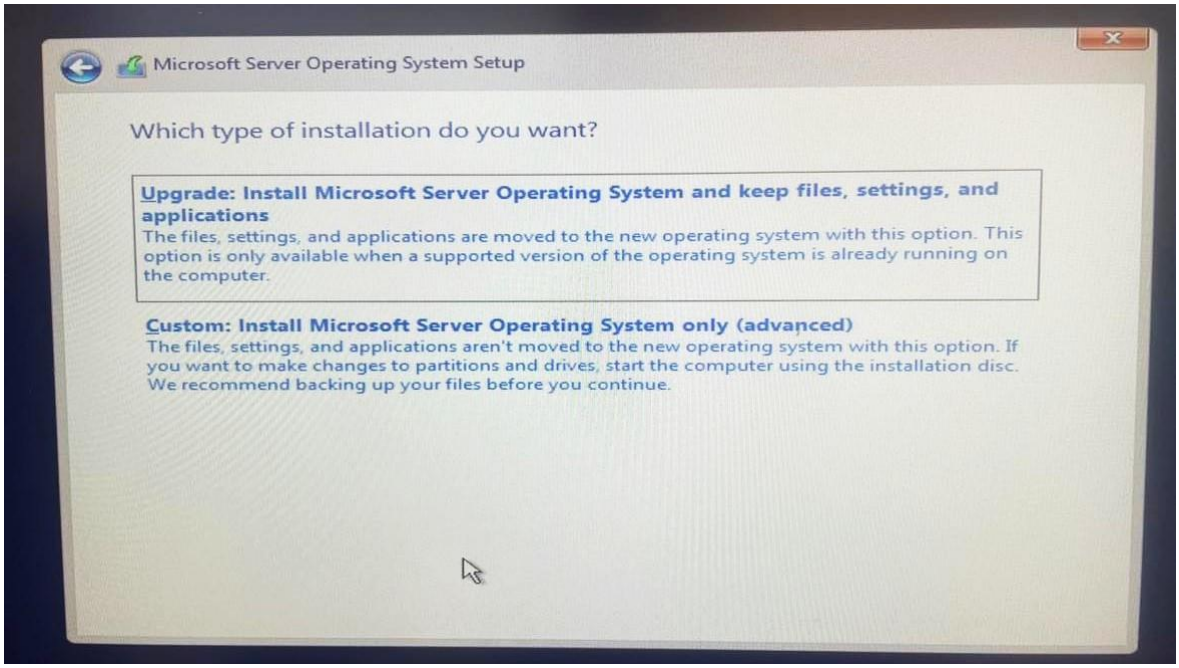
Obrázok 26 : Vloženie product key (vlastný zdroj)

Nasleduje výber verzie – pokiaľ by bol operačný systém sťahovaný priamo zo stránok Microsoftu určených pre verejnosť, v tomto menu by sa objavili všetky verzie, ktoré súvisia s Windows Server 2022. V tomto prípade bola vybraná konkrétna verzia už pri sťahovaní z Azure education, takže na výber sú dve možnosti, vybraná bola verzia s Desktop Experience.



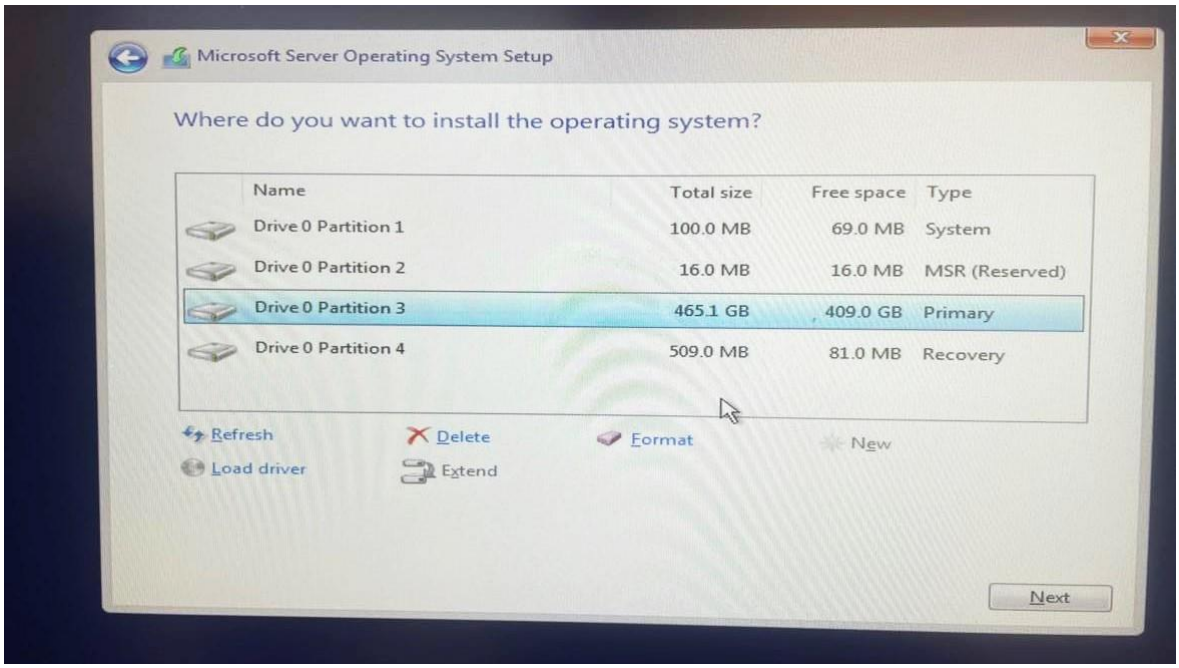
Obrázok 27 : Výber verzie inštalacie (vlastný zdroj)

Po tomto kroku je možné si z menu zvoliť, či sa má systém aktualizovať (táto možnosť sa využíva napríklad pri prechode na vyššiu verziu), alebo je možnosť si zvoliť čistú inštaláciu systému (táto možnosť bola zvolená).

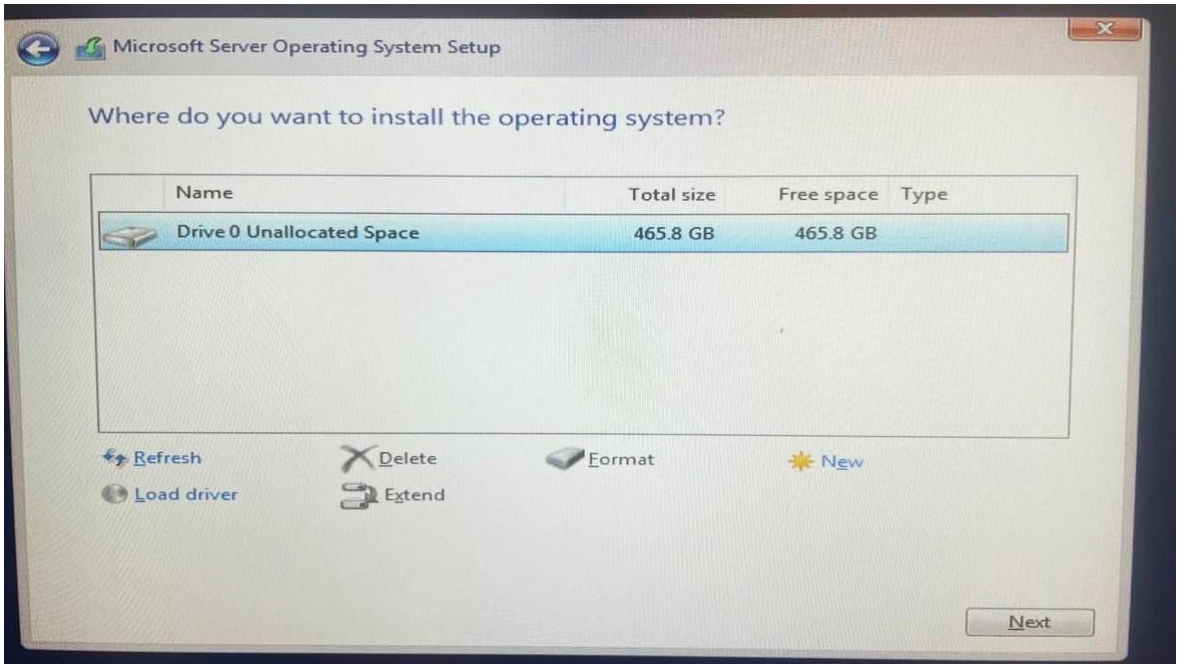


Obrázok 28 : Výber inštalácie systému (vlastný zdroj)

Nasleduje možnosť vybrať si, kam sa má operačný systém nainštalovať. Keďže na tomto počítači je ešte stále pôvodný operačný systém Windows 10 Pro, je potrebné kompletne všetky oddiely manuálne odstrániť

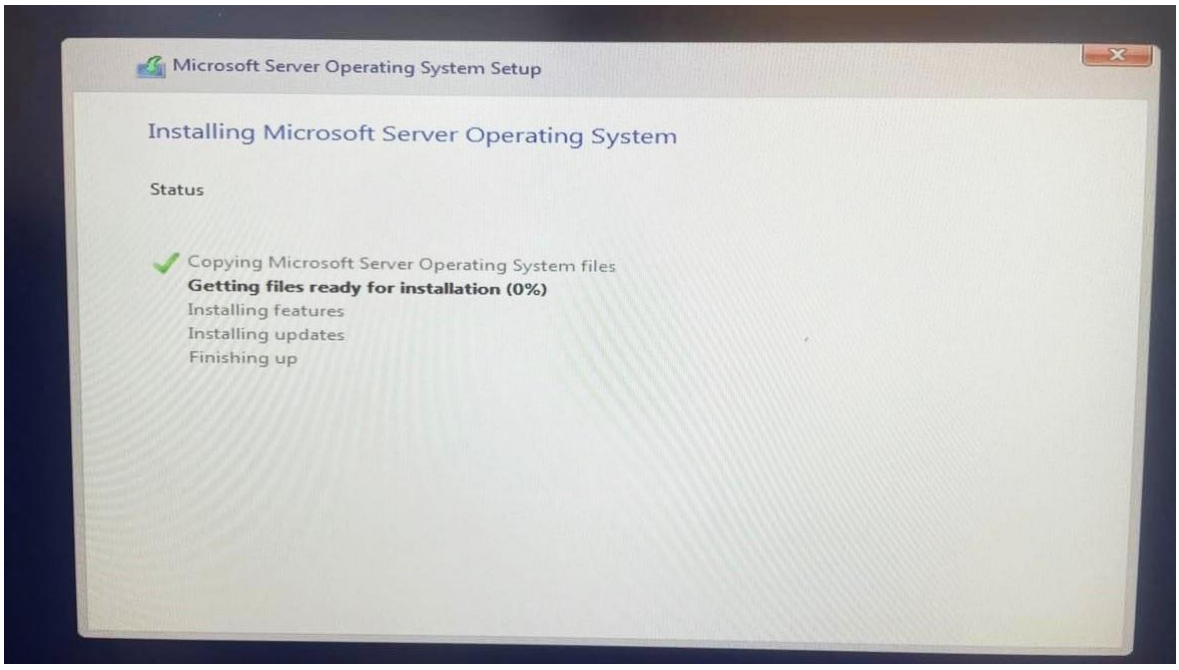


Obrázok 29 : Odstránenie nepotrebných oddielov (vlastný zdroj)



Obrázok 30 : Výber celého disku (vlastný zdroj)

Po tomto kroku sa začne systém inštalovať, stačí počkať na dokončenie a následný reštart systému.



Obrázok 31 : Inštalácia systému (vlastný zdroj)

5.2 Príprava počítača pred povýšením na doménový radič

V tomto stave je operačný systém Windows Server 2022 plne nainštalovaný, to však nestačí na to, aby sa stal doménovým radičom.

Predom je dôležité spomenúť fakt, že doménové radiče sú veľmi citlivé aj na zmeny, ktoré sa z užívateľského hľadiska nezdajú byť až takým veľkým zásahom do systému.

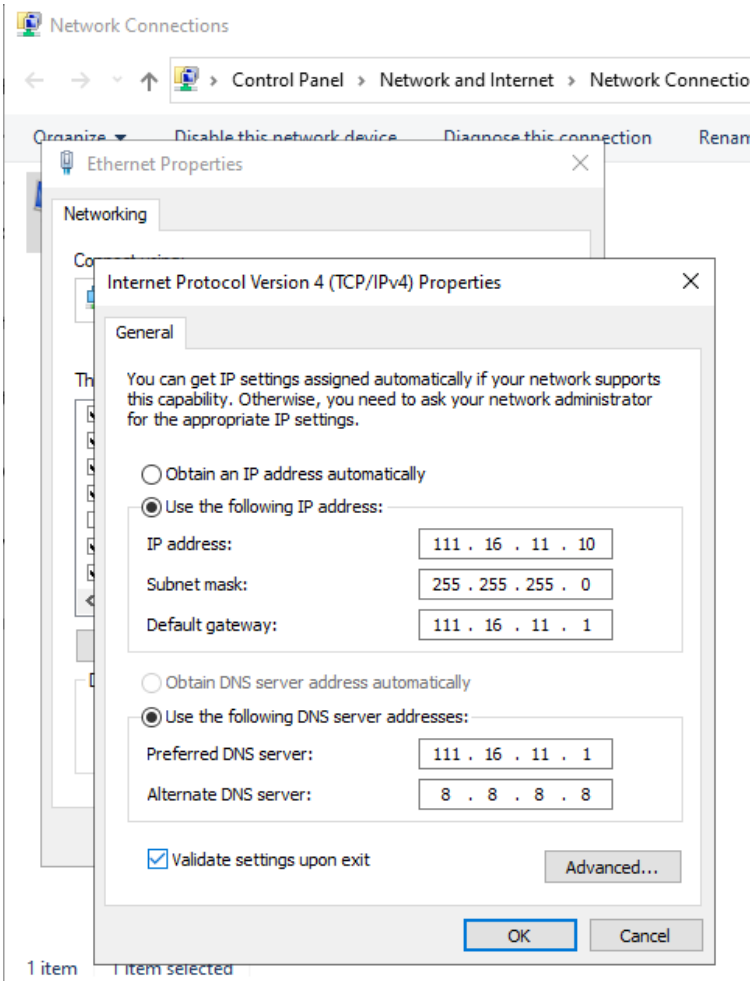
5.2.1 Nastavenie statickej IP adresy a názvu počítača

Doménový radič je server, ku ktorému pristupujú klientské stanice v sieti so svojimi požiadavkami. Keby sa IP adresa doménového radiča neustále menila vplyvom DHCP, server by nefungoval spoľahlivo a bol by obmedzený na funkcionalite (napríklad by nemohol plniť funkciu DNS serveru) atď.

IP adresa, ktorá sa pridelí doménovému radiču (zatiaľ ešte počítač nie je doménovým radičom) už ostane nemenná – pokiaľ by bola zmenená, rozbije sa konfigurácia, tým pádom server prestane spoľahlivo fungovať.

Aby sa mohla radiču prideliť statická IP adresa, najprv je potrebné zistiť, ktorá adresa v existujúcej sieti je voľná. Toho sa dá docieliť napríklad stiahnutím programu Angry IP Scanner, ktorý skenuje celý rozsah siete a označuje IP adresy farebne podľa toho, či patria nejakému zariadeniu. Tento program funguje na princípe sieťového príkazu ping (zariadenia označuje na základe toho, či z adresy príde odpoveď).

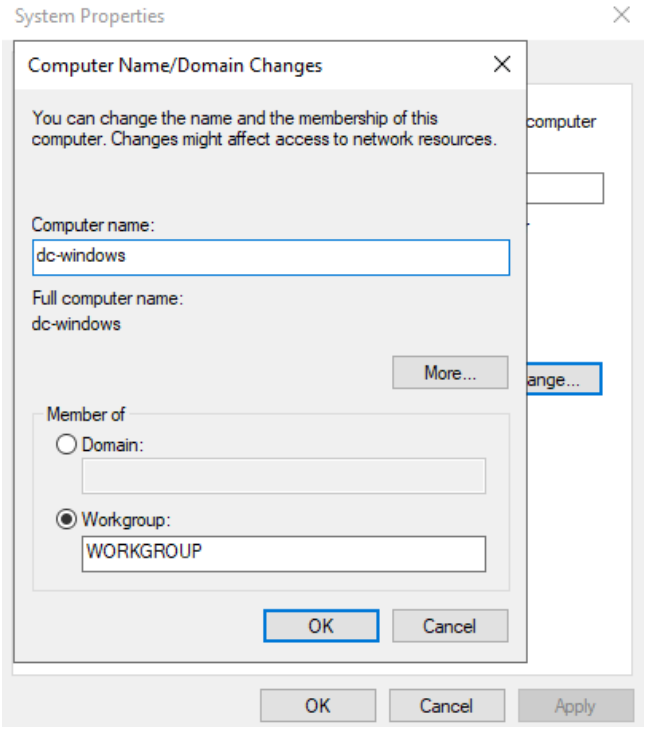
Statická IP adresa sa na počítači nastavuje v sieťových nastaveniach (v tomto prípade v „Network and Internet Settings“) v nastaveniach adaptéru. IP adresa pre Windows doménový radič bude 111.16.11.10, s tým že IP adresa DNS serveru a brány bude zatiaľ adresa routra (ktorý medzitým plní aj úlohu DHCP serveru).



Obrázok 32 : Nastavenie statickej IP adresy (vlastný zdroj)

Správnosť konfigurácie sa dá overiť pomocou príkazového riadku a príkazom ipconfig /all, ktorý vypíše informácie o sieťových pripojeniach. Tento krok však môže byť bez problémov preskočený.

Ďalším potrebným nastavením je zmena názvu počítača. Toto nastavenie sa schováva pod nastavením systému v záložke informácií. Nastavený nový názov počítača je „dc-windows“



Obrázok 33 : Zmena názvu počítača (vlastný zdroj)

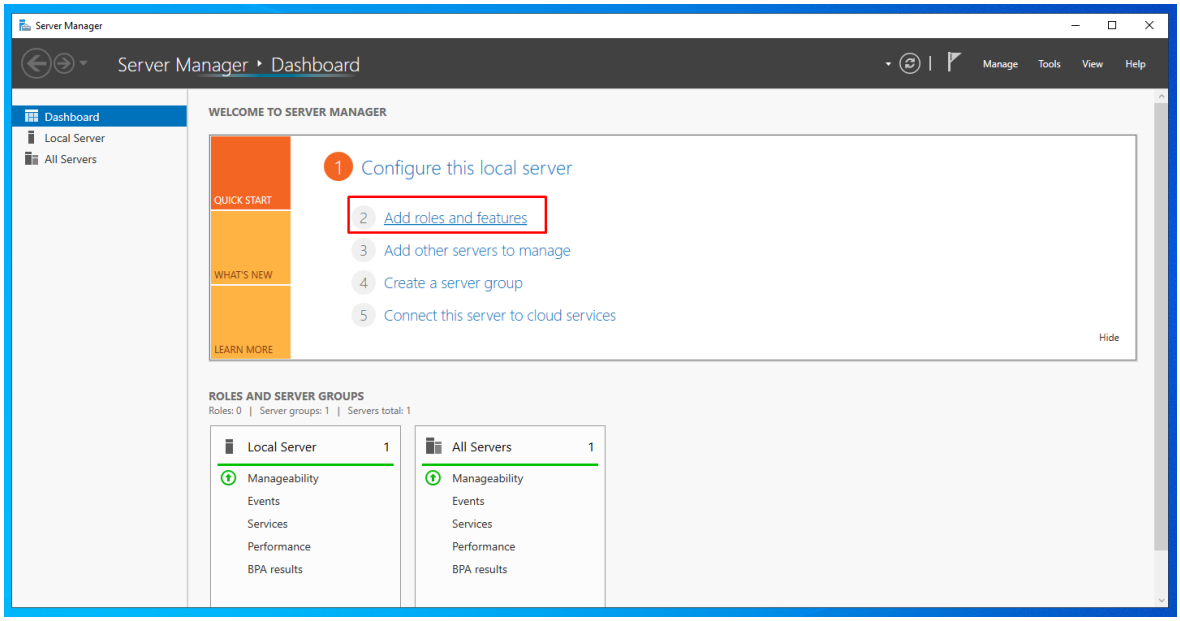
Týmto krokom sa zavŕšili prípravy na povýšenie počítača na doménový radič.

5.3 Inštalácia a konfigurácia rolí a funkcií

Role a funkcie sa najprv musia nainštalovať a následne prebieha ich konfigurácia. Role a funkcie sa dajú inštalovať hromadne, čo v tejto diplomovej práci bude využité, aby zanikla nutnosť popisovať inštaláciu každej role a funkcie samostatne.

Taktiež je dôležité poznamenať, že funkcie nepotrebujú na rozdiel od rolí konfiguráciu, stačí ich len nainštalovať.

Aby mohla inštalácia započať, je potrebné si otvoriť „Server Manager“, ktorý je v podstate centrom riadenia doménového radiča. Na ľavej lište sa nachádzajú položky: Dashboard, Local Server, All servers – pokiaľ by už boli nainštalované ľubovoľné služby, zobrazia sa tam tiež. Momentálne je dôležitá lišta Dashboard, ktorá ponúka možnosť inštalácie rolí a funkcií.



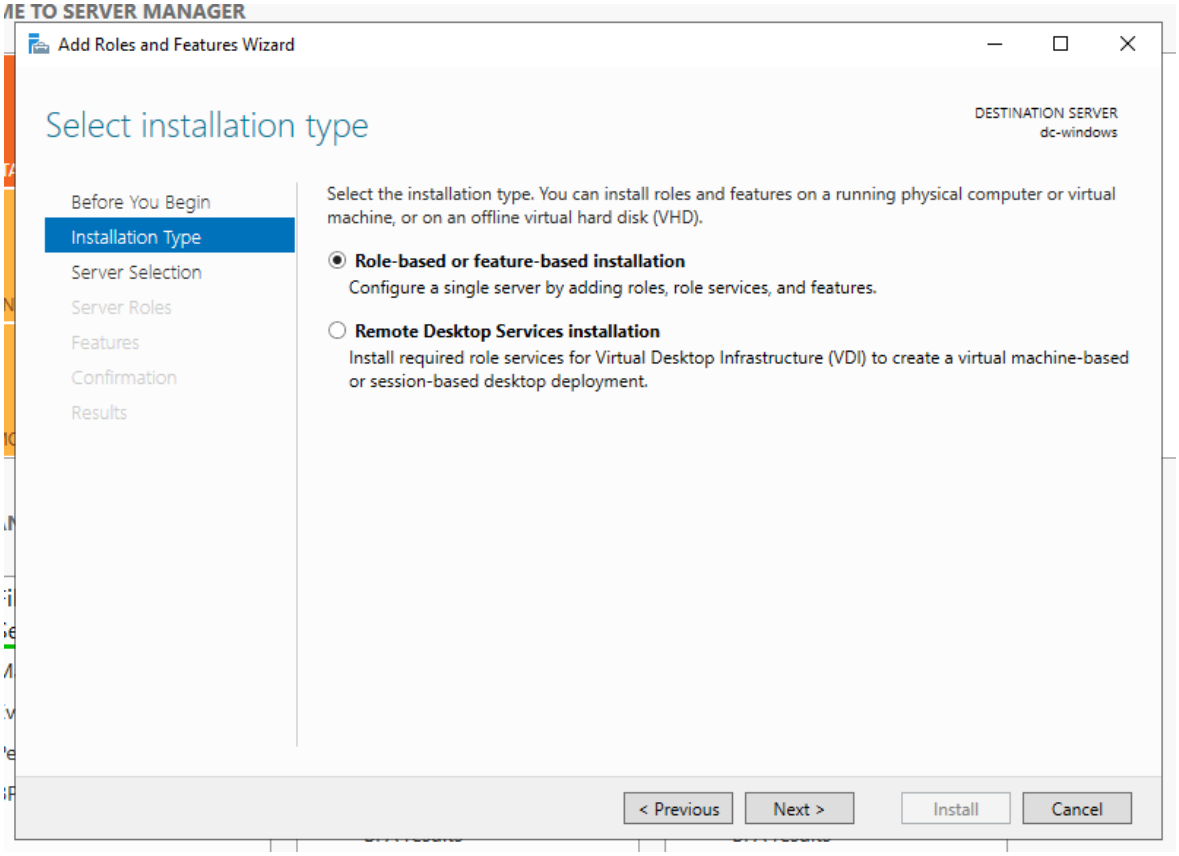
Obrázok 34 : Inštalácia rolí a funkcií (vlastný zdroj)

Po kliknutí na „Add roles and features“ sa zobrazí sprievodca inštaláciou. Úvodná stránka obsahuje základné informácie, takže sa preskočí a inštalácia rolí a funkcií môže byť zahájená.

Po úvodnej stránke sa sprievodca opýta na typ inštalácie. Inštalácia rolí a funkcií môže byť buď:

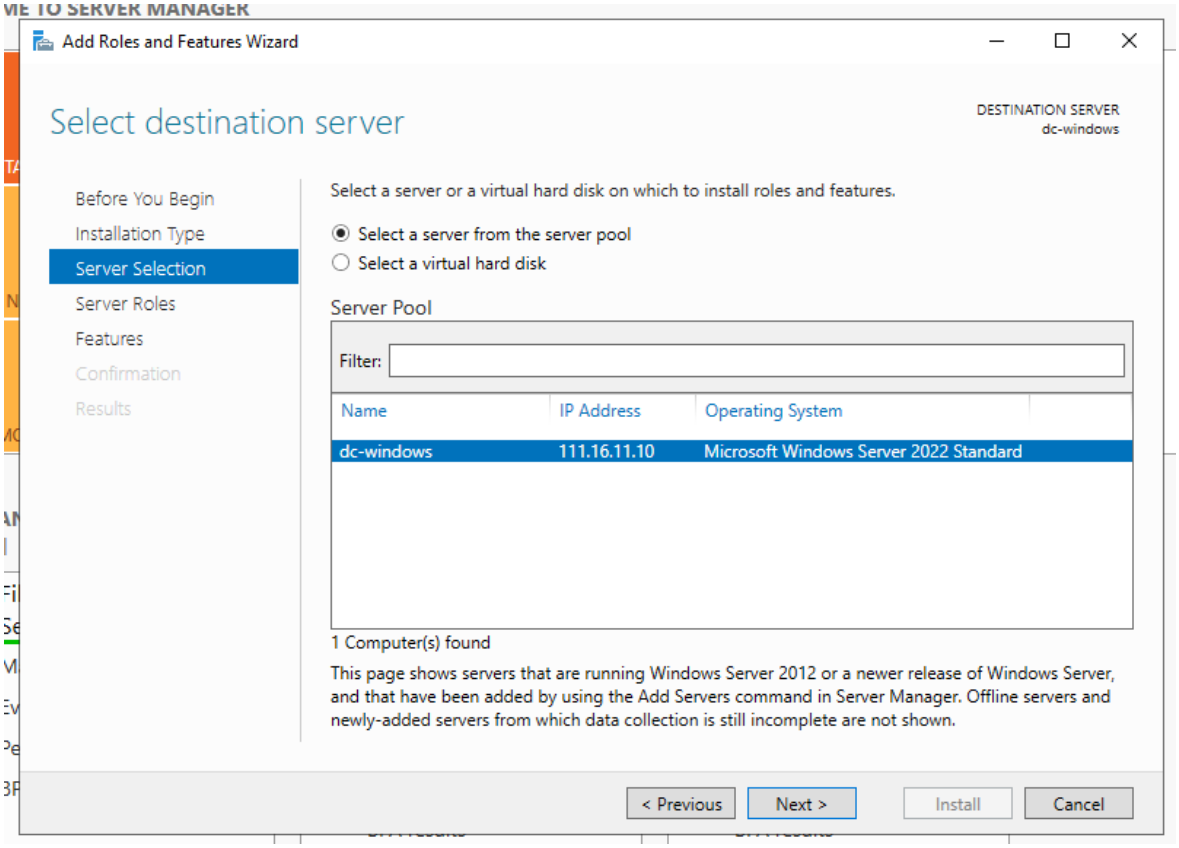
- Na fyzickom zariadení
- Na virtuálnom zariadení
- Na offline VHD

V tomto prípade to bude inštalácia na fyzickom zariadení.



Obrázok 35 : Výber typu inštalácie (vlastný zdroj)

Po tomto kroku nasleduje výber serveru alebo VHD, kde sa role a funkcie budú inštalovať. Keďže fyzické zariadenie (radič) je v sieti len jeden, vyberie sa ten.

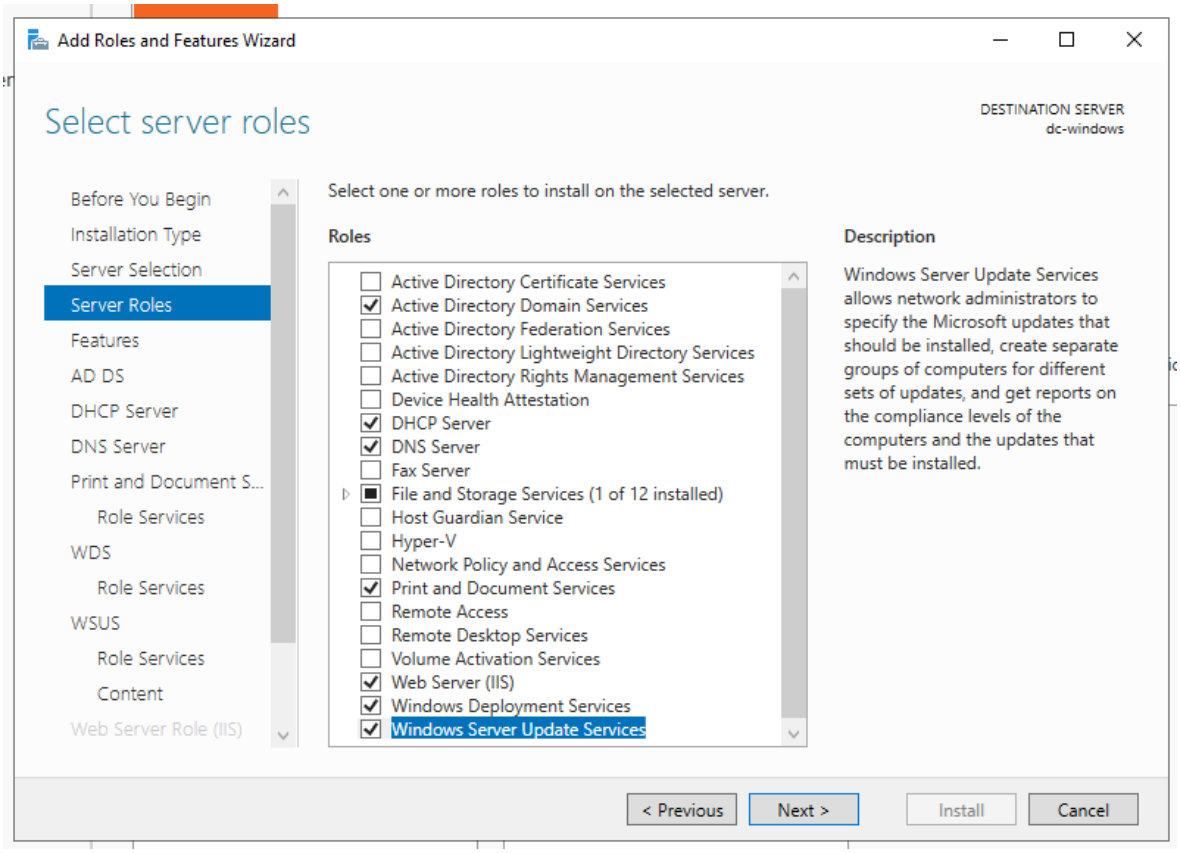


Obrázok 36 : Výber servera pre inštaláciu rolí s funkcií (vlastný zdroj)

Po tomto kroku nasleduje výber rolí, vybrané budú nasledujúce role:

- Active Directory Domain Services
- DNS Server
- DHCP Server
- Print and Document Services
- Windows Server Update Services

Tieto role sú vybrané, avšak pri inštalácii role WSUS sa automaticky zaškrtne aj políčko pre inštaláciu role Web Server. Okrem toho pri výbere funkcie BitLocker Network Unlock sa automaticky zaškrtne políčko pre inštaláciu role Windows Deployment Services.

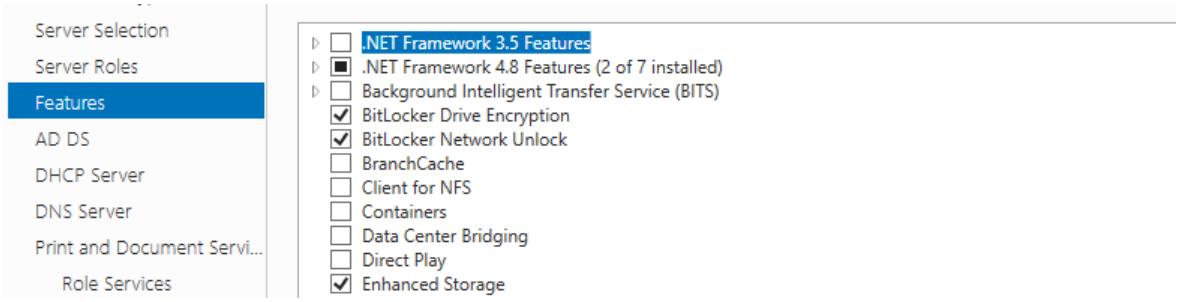


Obrázok 37 : Výber rolí (vlastný zdroj)

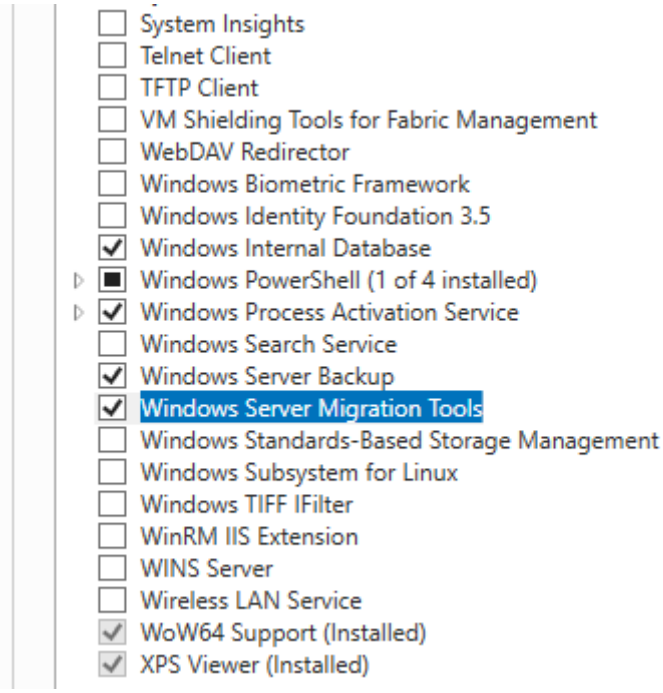
Po výbere rolí nasleduje výber funkcií, vybrané budú nasledujúce funkcie:

- BitLocker Drive Encryption
- BitLocker Network Unlock
- Windows Server Backup
- Windows Server Migration Tools

Tak, ako to bolo pri rolách, tieto funkcie boli vybrané, avšak pri inštalácii role Active Directory Domain Services sa automaticky zaškrtne políčko pre inštaláciu funkcií Group Policy Management a Remote Server Administration Tools. Pri inštalácii role WSUS sa automaticky zaškrtne políčko pre inštaláciu funkcií Windows Internal Database a Windows Process Activation Service.



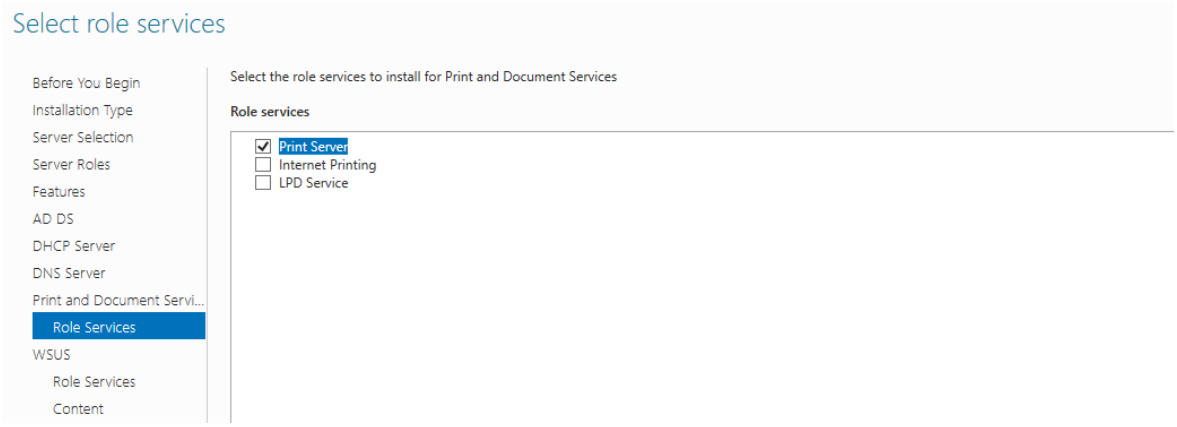
Obrázok 38 : Výber funkcií 1 (vlastný zdroj)



Obrázok 39 : Výber funkcií 3 (vlastný zdroj)

Po tomto výbere je potrebné u niektorých rolí vybrať služby, týka sa to rolí: Print and Document Services, Windows Server Update Services (tu je ešte potrebné okrem výberu služieb špecifikovať, kde budú aktualizácie ukladané), Web server a Windows Deploy Services.

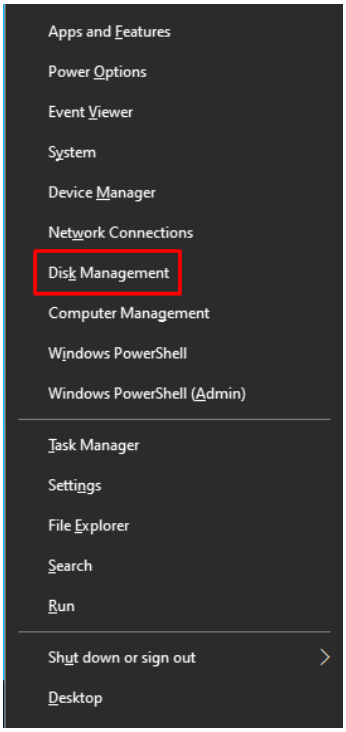
Pri výbere služieb role Print and Documents Services sú na výber tri možnosti, zvolená bude možnosť Print Server.



Obrázok 40 : Výber služieb role Print and Document Services (vlastný zdroj)

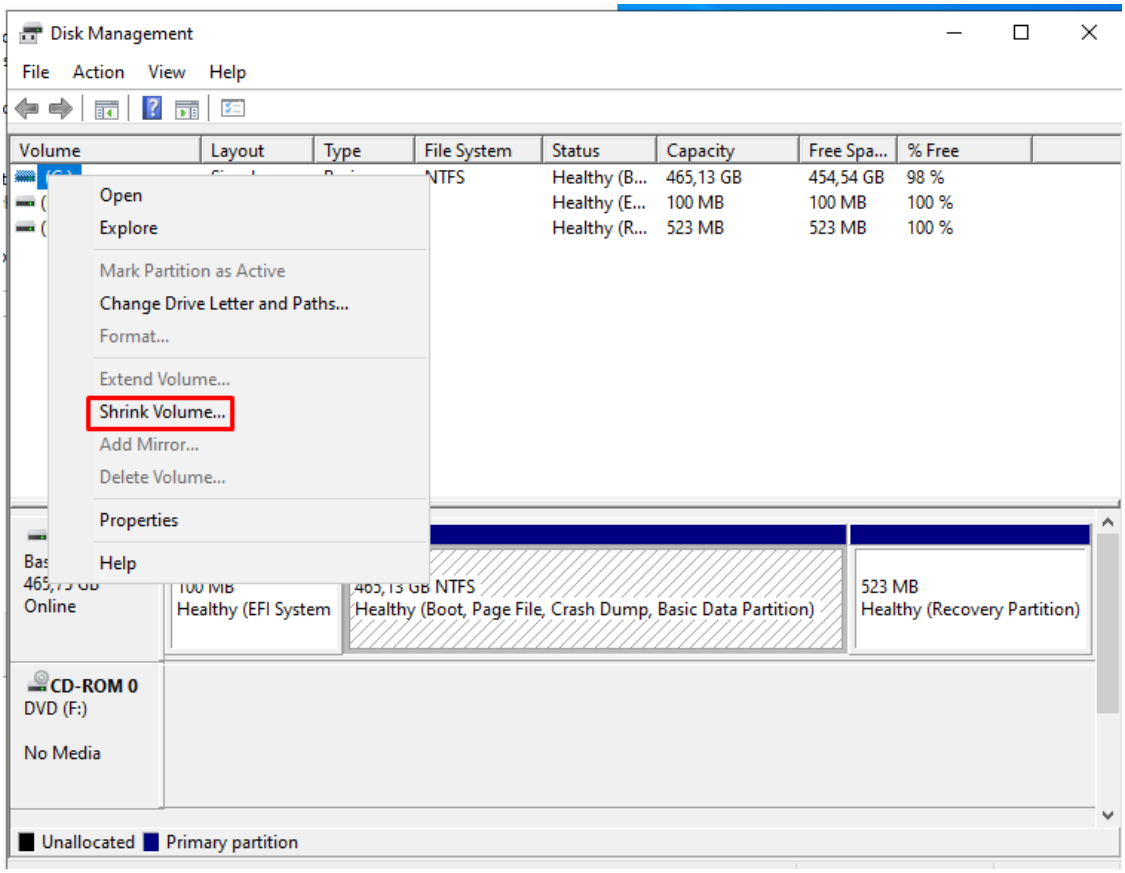
Nasleduje výber služieb role WSUS. Tu je potrebné urobiť ešte pár medzikrokov – konkrétne vyhradiť miesto na disku, kde sa budú ukladať aktualizácie pre WSUS, začne sa teda týmito krokmi.

Kombináciou tlačidiel win+x sa otvorí menu, z ktorého sa zvolí možnosť „Disk Management“.



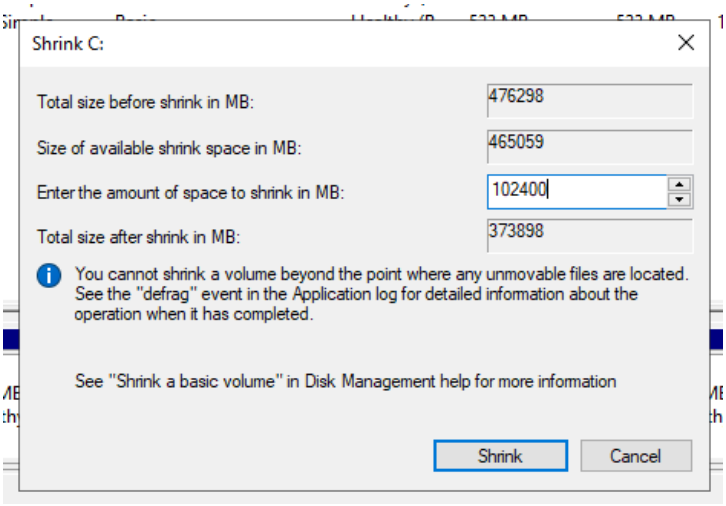
Obrázok 41 : Zapnutie konzole Disk Management (vlastný zdroj)

Vo zväzkoch sa nachádzajú zväzok C: a dva zväzky vyhradené pre systém – je teda potrebné odobrať miesto z disku C: a následne toto odobrané miesto naformátovať a vhodne pomenovať.



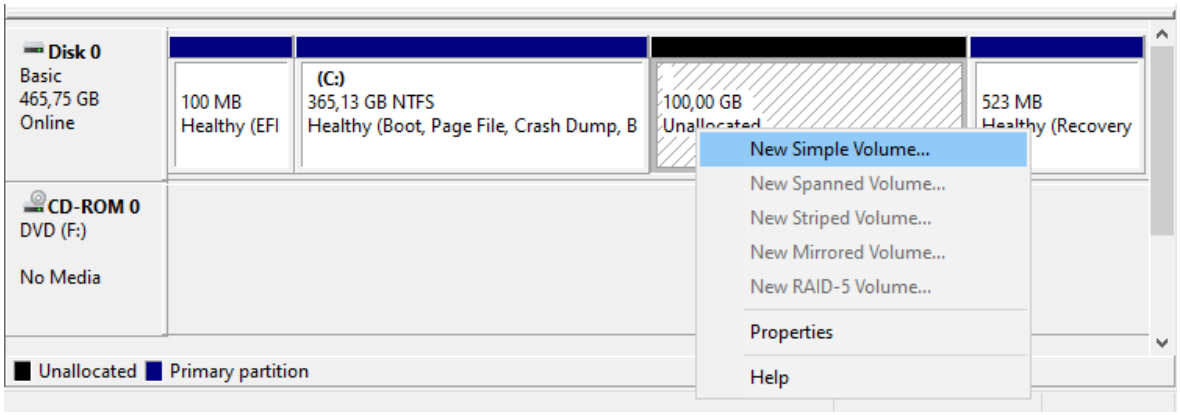
Obrázok 42 : Odobratie kapacity zo zväzku C: (vlastný zdroj)

Pre testovacie účely stačí pre WSUS odobrať napríklad 100 GB kapacity.



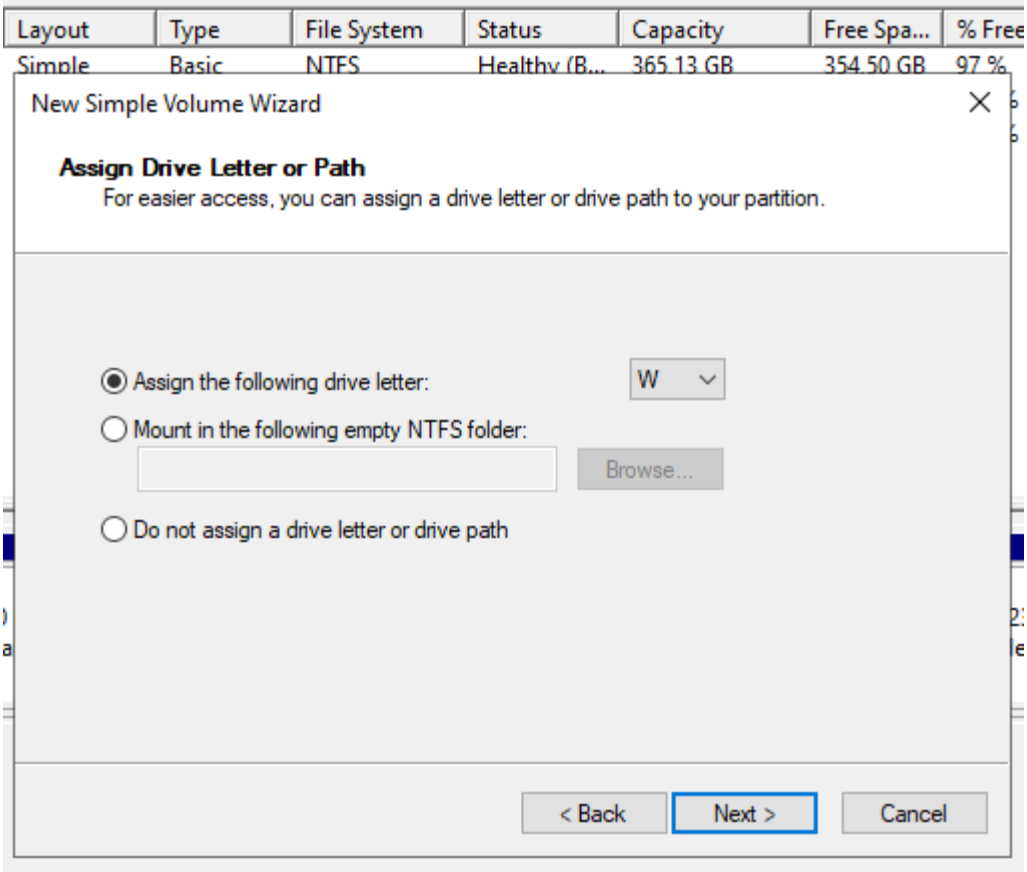
Obrázok 43 : Odobratie kapacity 100 GB zo zväzku C: (vlastný zdroj)

Miesto, ktoré sa odoberie je vedené ako nealokované, čiže je potrebné z neho vytvoriť nový zväzok.



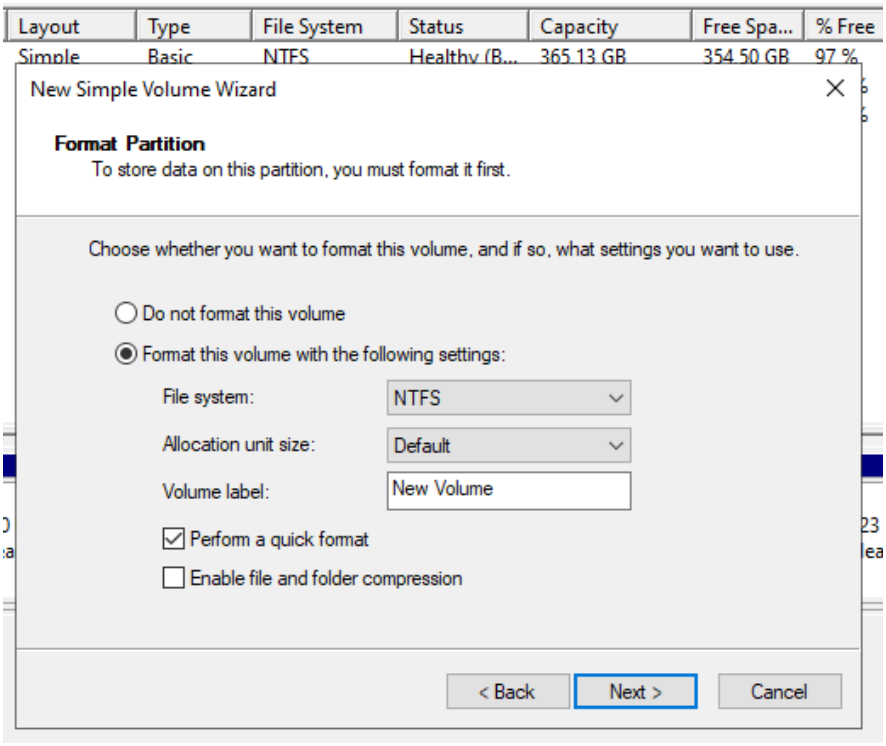
Obrázok 44 : Vytvorenie nového zväzku (vlastný zdroj)

Následne sa otvorí sprievodca nastavení nového zväzku, písmeno pre zväzok bolo zvolené „W“, ako WSUS.



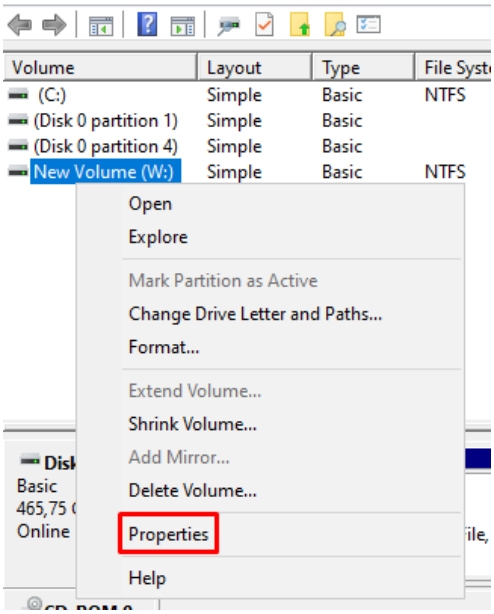
Obrázok 45 : Obrázok 37: Zvolenie písmena zväzku (vlastný zdroj)

Potom je potrebné nastaviť formátovanie, zvolené bolo formátovanie NTFS.



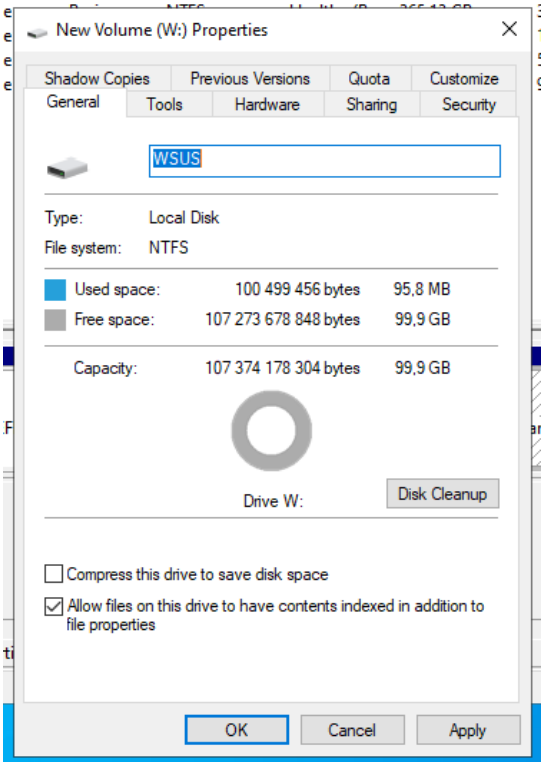
Obrázok 46 : Zvolenie formátovania (vlastný zdroj)

Následne sa zväzok ešte premenuje – aby bolo jasné, na čo slúži, teda čo sa v ňom bude nachádzať. Stačí kliknúť pravým tlačidlom na zväzok a zvoliť možnosť „Properties“.



Obrázok 47 : Nastavenia zväzku (vlastný zdroj)

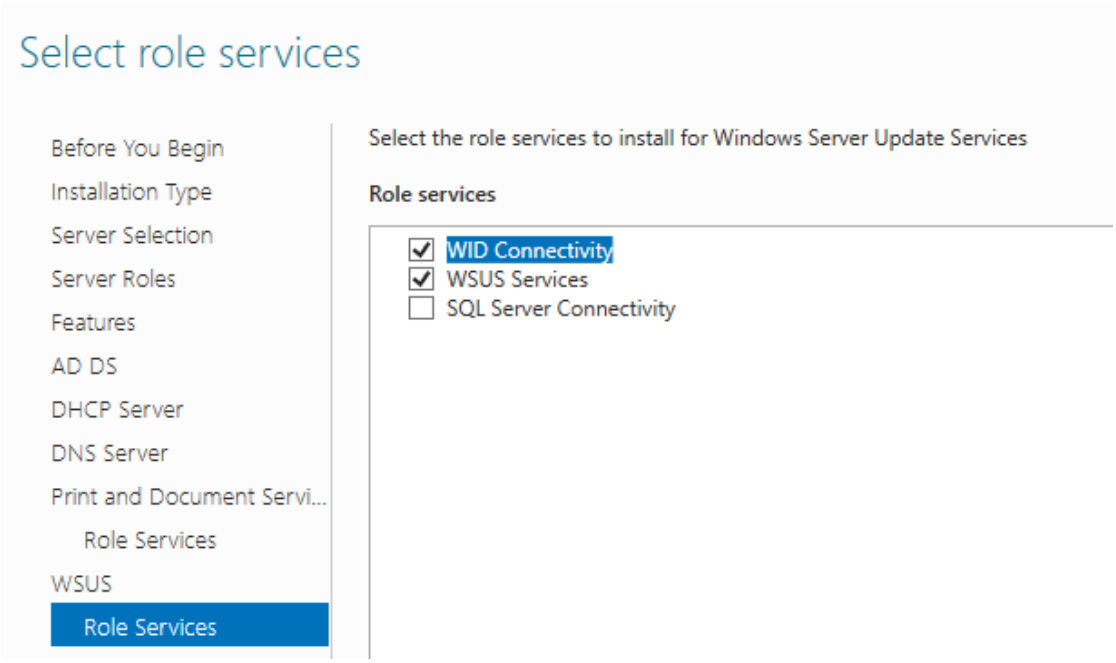
Samotná zmena názvu zväzku sa nachádza na záložke „General“, kde teda ako názov bude vyplnený „WSUS“



Obrázok 48 : Zmena názvu zväzku (vlastný zdroj)

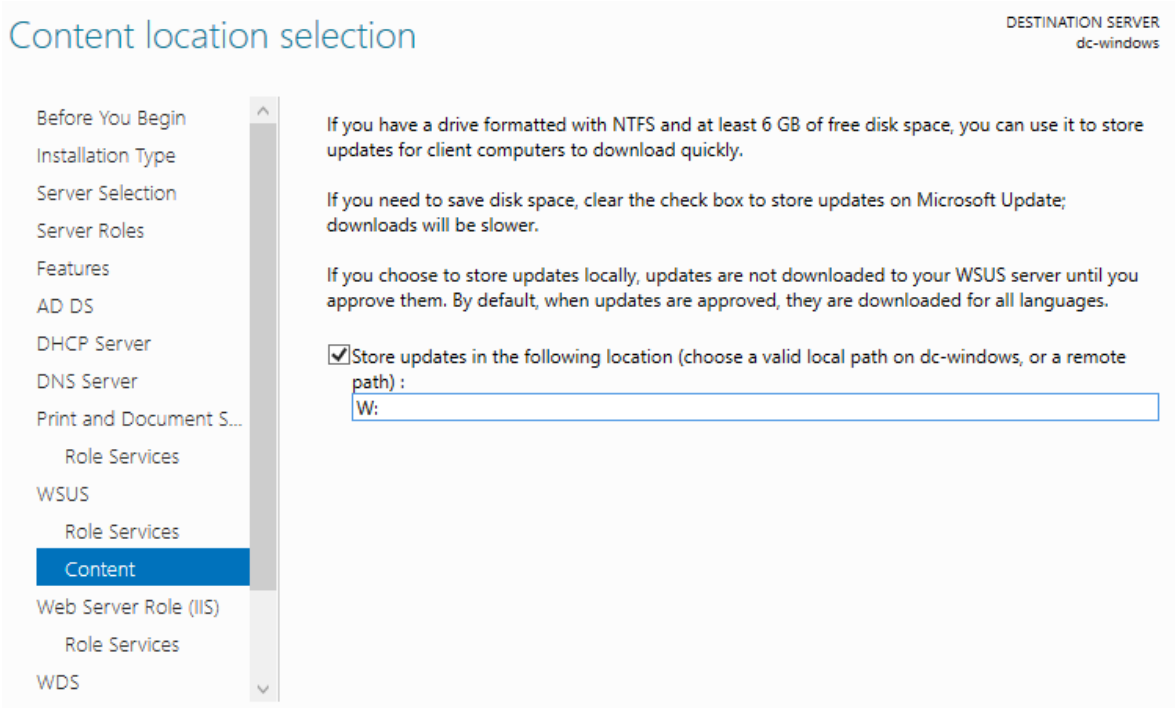
Týmto sa dokončilo nastavenie vyhradenie miesta pre aktualizácie WSUS, takže môže pokračovať nastavenie výberu služieb role WSUS.

Vybrané sú služby WID Connectivity a WSUS Services, na tom nie je potrebné nič meniť, ani pridávať.



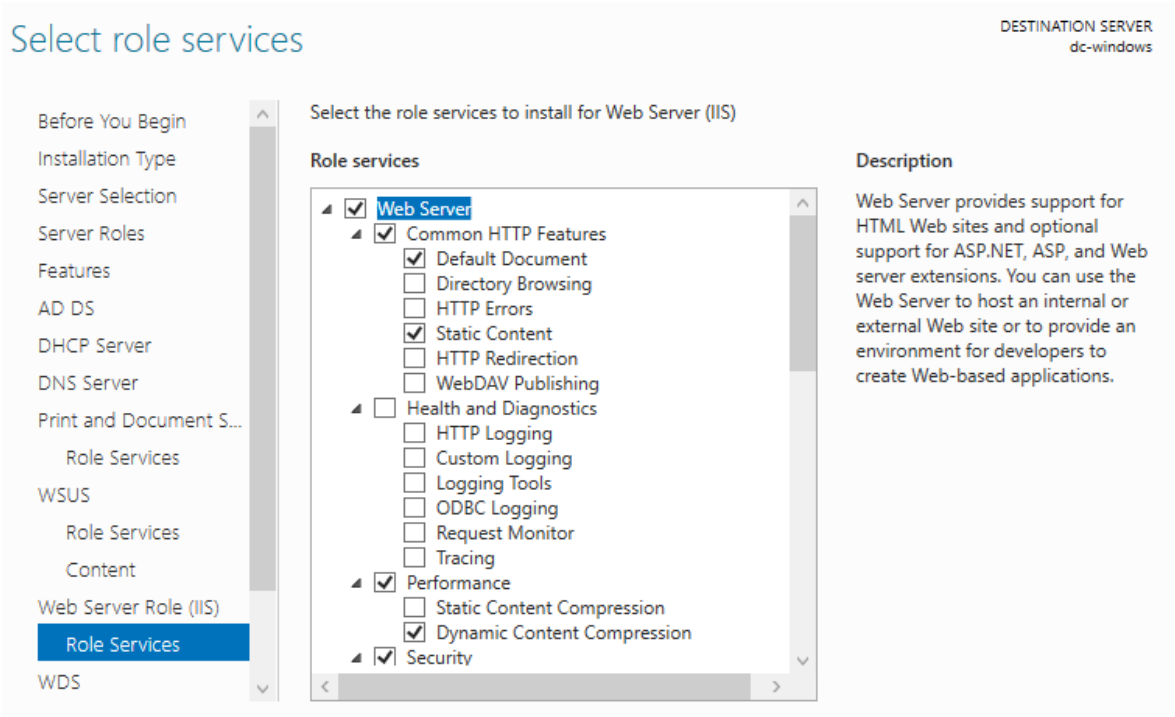
Obrázok 49 : Výber služieb role Windows Server Update Services (vlastný zdroj)

Hneď po výbere rolí nasleduje nastavenie cesty, ktorá povedie na lokalitu, kde sa budú ukladať aktualizácie. V tomto prípade je to veľmi jednoduché, keďže bol pre tento účel priamo vytvorený zväzok W:.



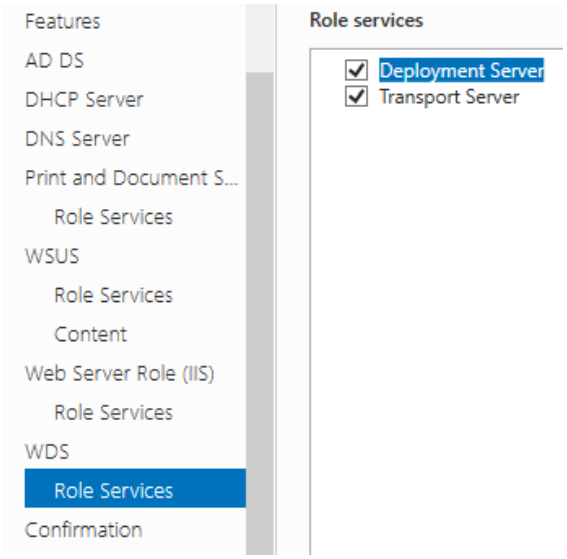
Obrázok 50 : Výber lokácie pre ukladanie aktualizácií (vlastný zdroj)

Nasleduje výber služieb role Web Server. Tu sú dané role zaškrtnuté, nie je potrebné ich nijak meniť.



Obrázok 51 : Výber služieb role Web Server (vlastný zdroj)

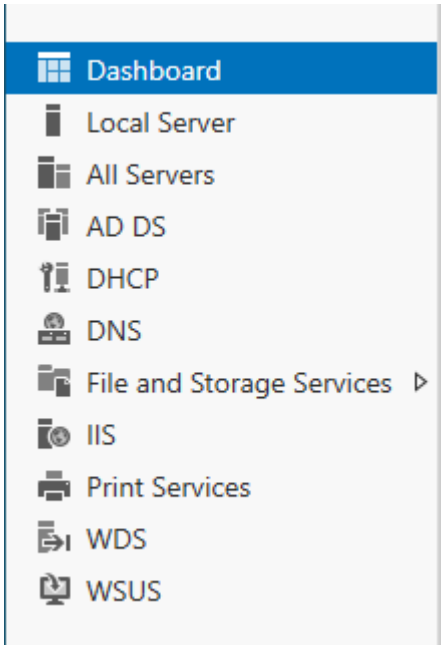
Ostáva ešte posledný výber služieb role Windows Deployment Services, kde sú zaškrnuté obe možnosti, ktoré nie je potrebné meniť.



Obrázok 52 : Výber služieb role Windows Deployment Services (vlastný zdroj)

V tejto chvíli sú vybrané všetky role, funkcie a služby, takže stačí sprievodcu inštaláciou dokončiť, počkať na nainštalovanie a reštartovať server.

Po reštarte vyzerá ľavá bočná lišta nasledovne (funkcie v dashboarde nie sú viditeľné).



Obrázok 53 : Ľavá bočná lišta po inštalácii (vlastný zdroj)

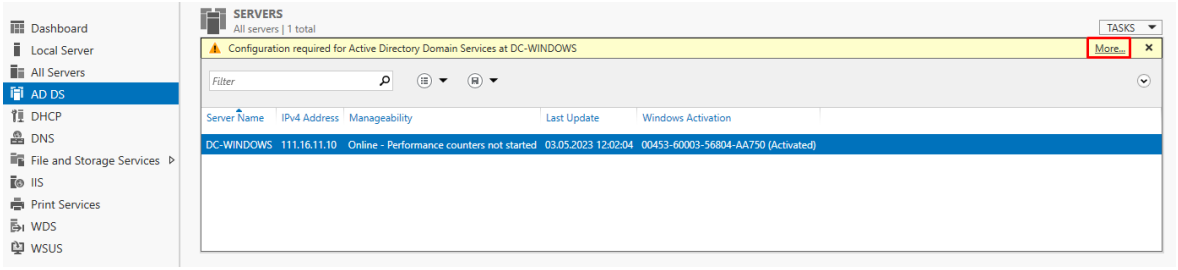
Ako bolo spomínané v teoretickej časti, role nie je potrebné len nainštalovať, ale po reštarte zariadenia je potrebná ich konfigurácia.

5.3.1 Konfigurácia role Active Directory Domain Services

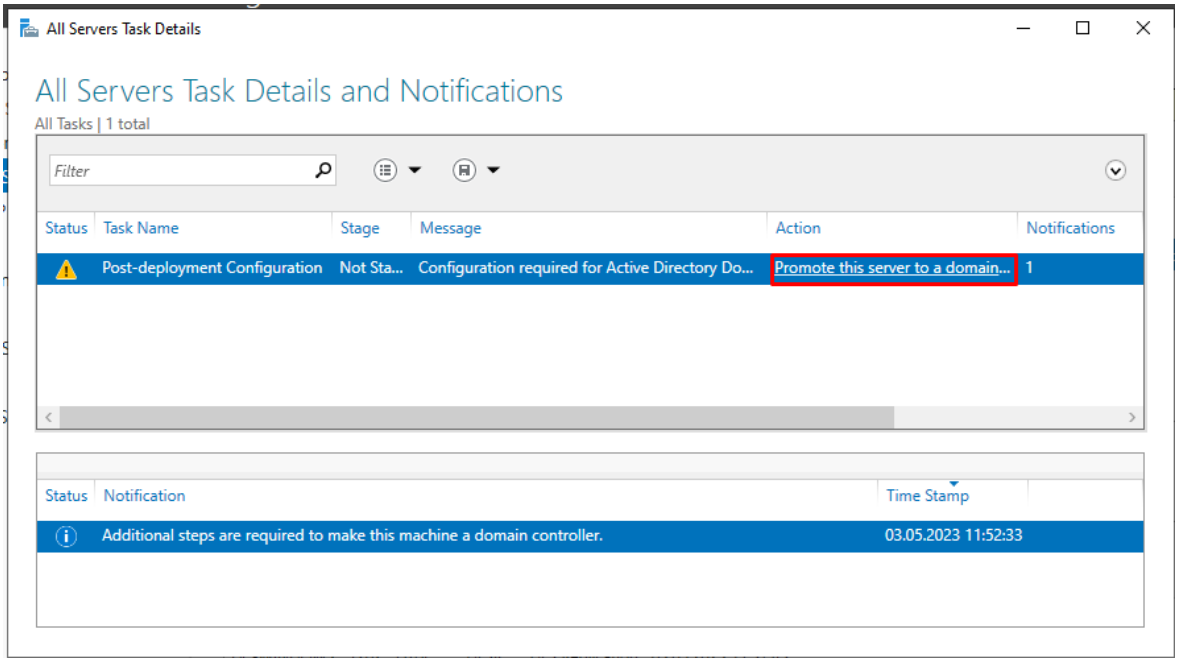
Najprv je potrebné začať konfiguráciou role Active Directory Domain Services. Táto rola je úplne základnou rolou, ktorá robí doménový radič doménovým radičom a bez nej by to jednoducho nešlo.

Na ľavej lište stačí na rolu kliknúť, po kliknutí je tam žltá lišta, ktorá upozorňuje na to, že je potrebné rolu nakonfigurovať. Po stlačení možnosti „More“ sa naskytne možnosť „Promote this server to a domain controller “, ktorá umožní povýšiť počítač na doménový radič.

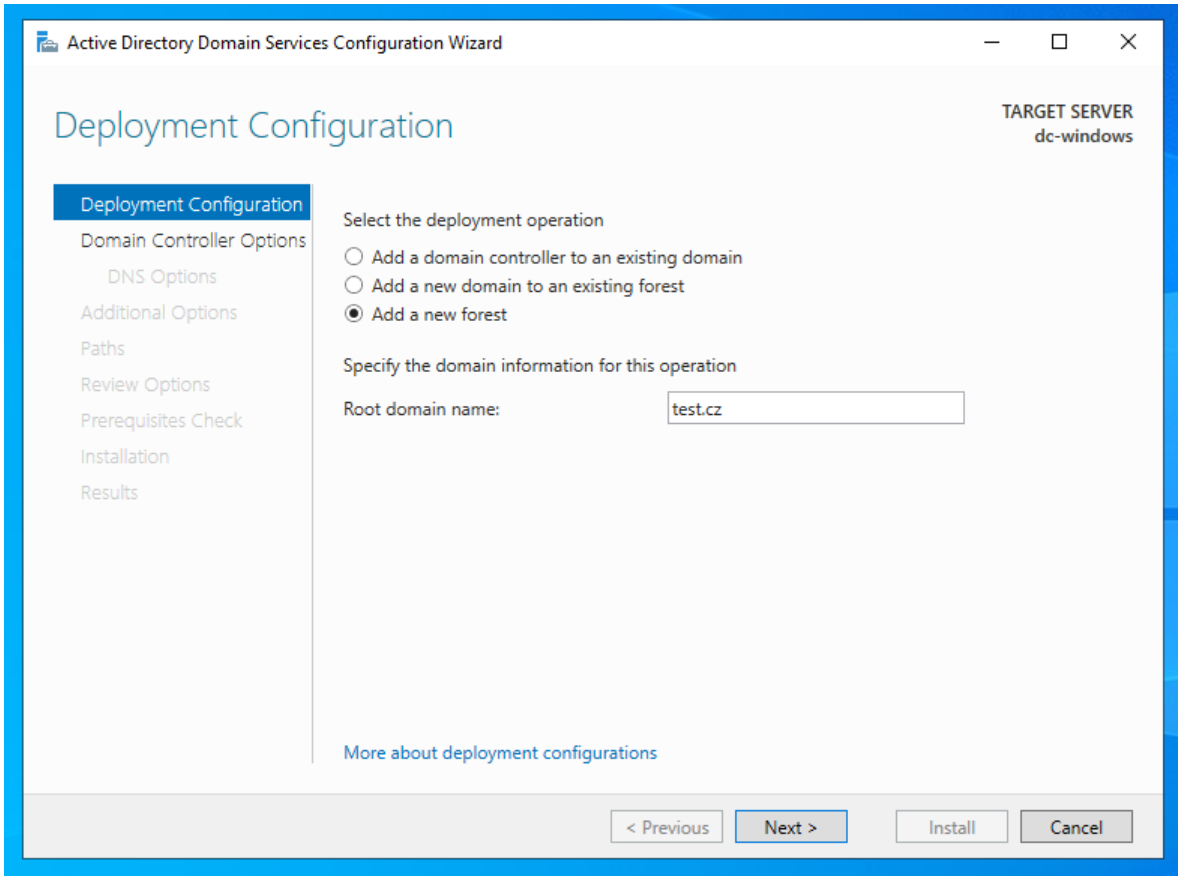
Po kliknutí na políčko povýšenia počítača na doménový radič sa zobrazí sprievodca pre konfiguráciu role. Ako prvé je potrebné vybrať, čo sa má so serverom udiať. Sú tam tri možnosti, bude vybraná „Add a new forest“, pretože žiadne iné domény ani lesy nakonfigurované nie sú. Zároveň je tam políčko pre vpísanie root domain name (teda koreňového doménového mena), čo v tomto prípade bude „test.cz“. Kedysi sa zvyklo RDN zadávať ako „doména.local“, čo už je dnes zastarané.



Obrázok 54 : Rozkliknutie konfigurácie (vlastný zdroj)

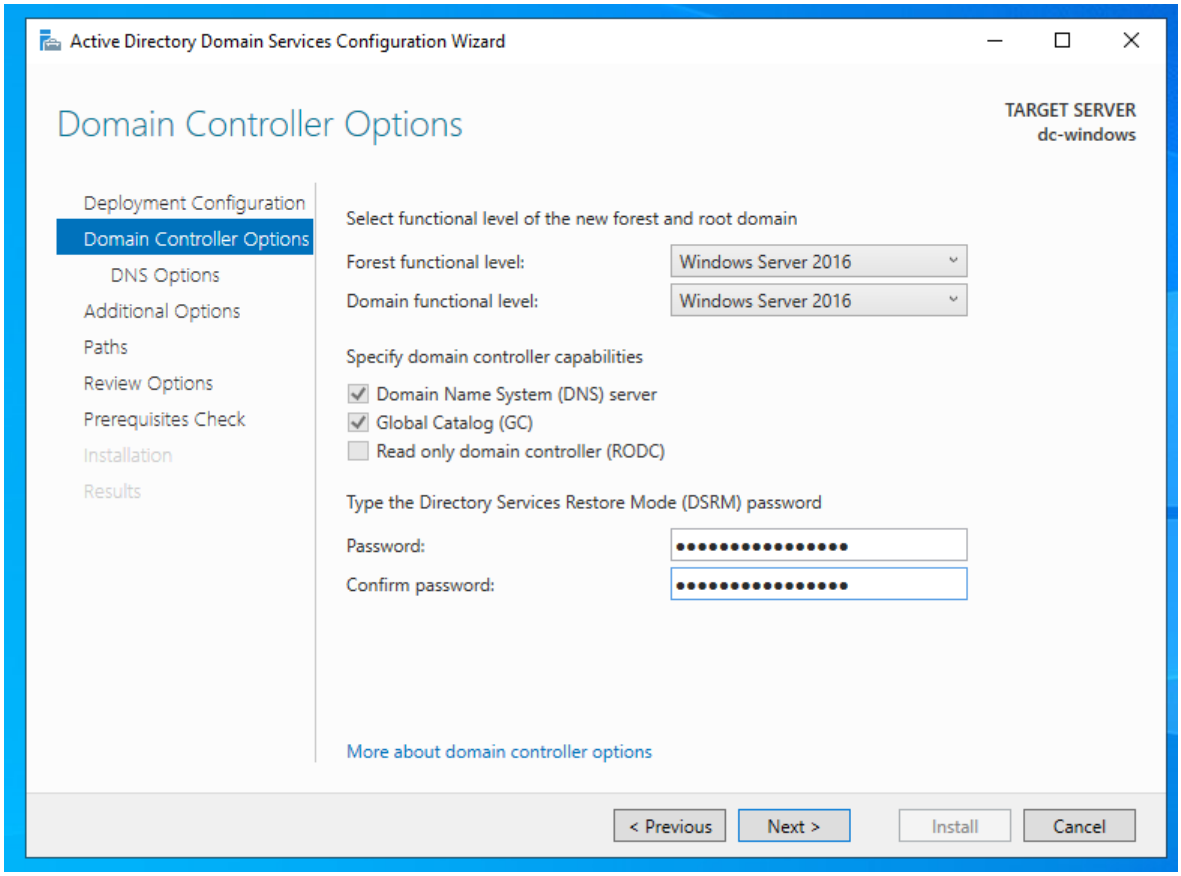


Obrázok 55 : Začiatok povýšenia počítača na doménový radič (vlastný zdroj)



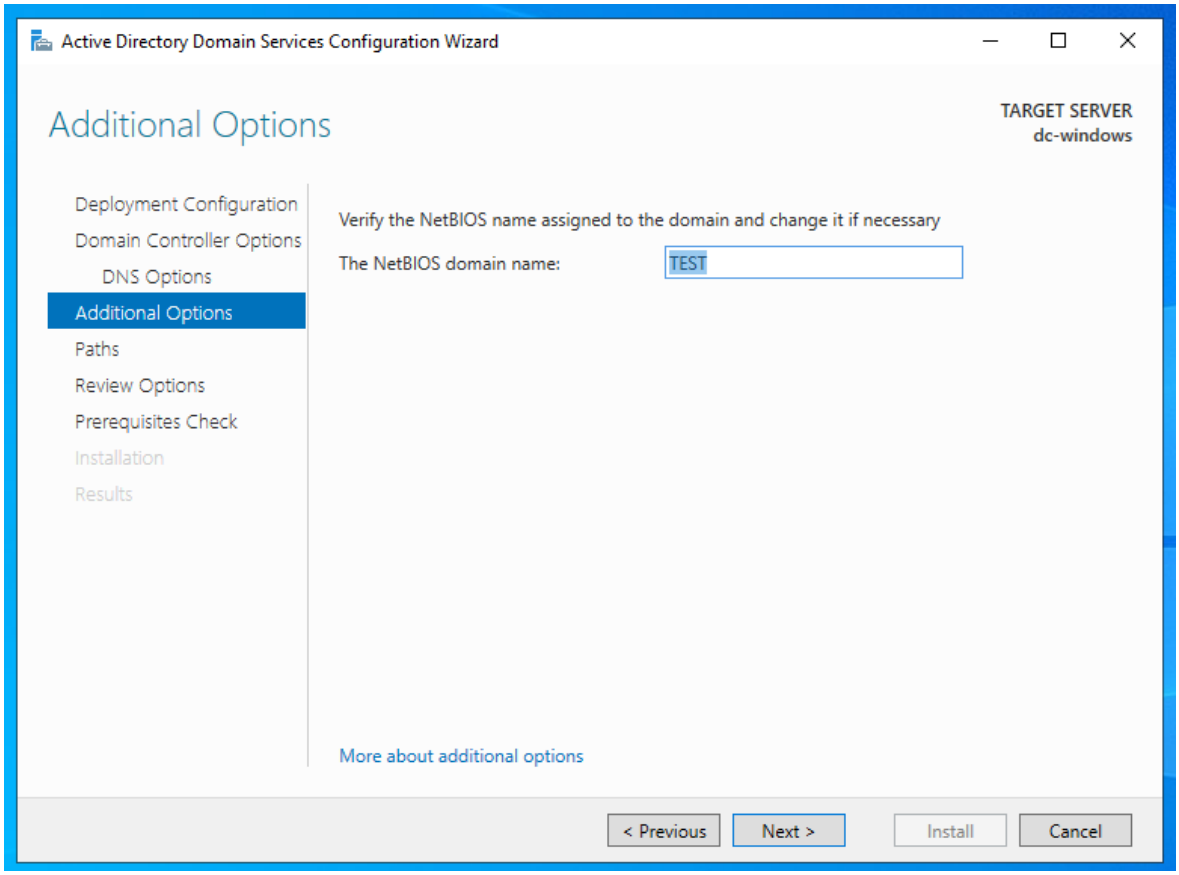
Obrázok 56 : Nastavenie deployment operation a root domain name (vlastný zdroj)

Nasledujú nastavenia týkajúce sa doménového radiča. Ako prvé sa nastavuje level funkcionality, ktorý bude nastavený na najvyšší (v tomto prípade Windows Server 2016), nasleduje nastavenie schopností radiča (jediné, čo v tomto prípade nie je potrebné je RODC) a ako posledné je potrebné nastaviť DSRM heslo. DSRM heslo poskytuje administrátorovi zadné vrátka k databázam, preto je dôležité ho vhodne vybrať a nestratiť.



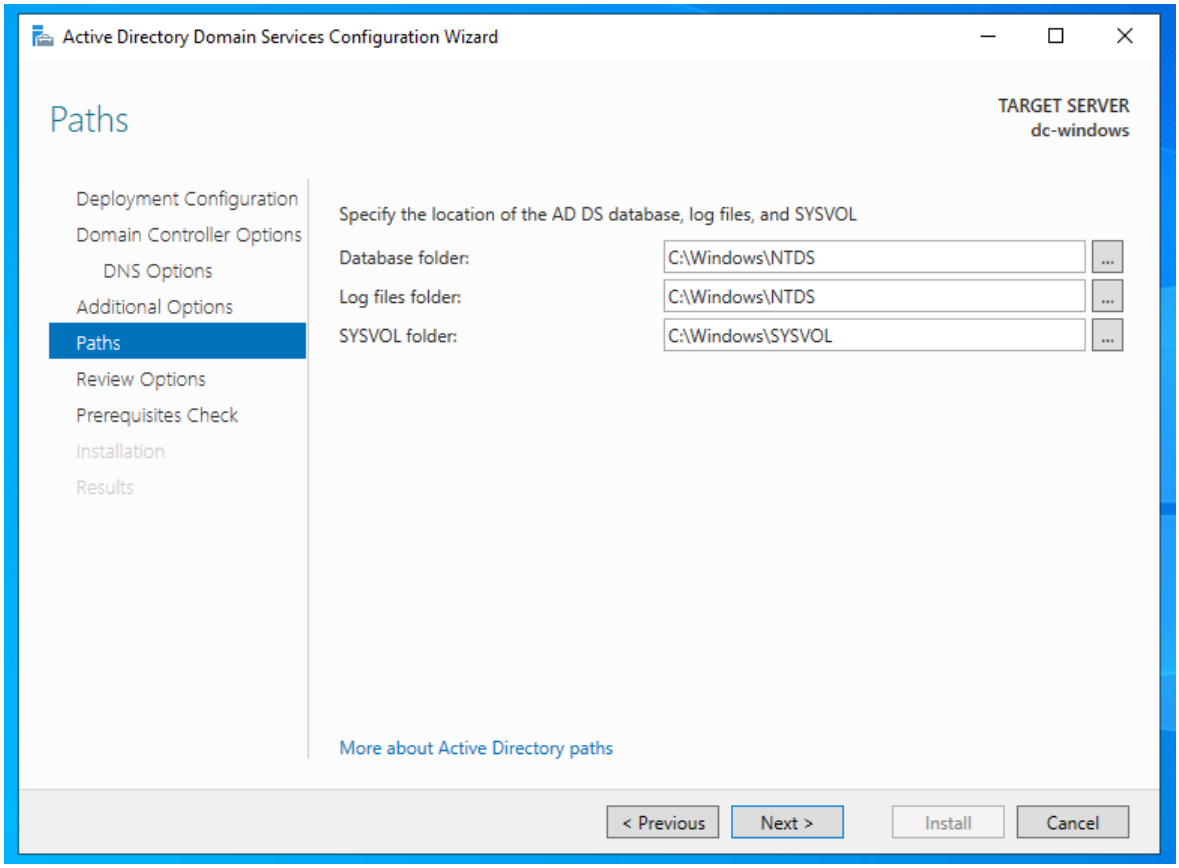
Obrázok 57 : Nastavenia doménového radiča (vlastný zdroj)

Sprievodca ďalej naviguje na nastavenia DNS. Keďže DNS rola zatiaľ nie je nakonfigurovaná, tento krok sa môže preskočiť bez spôsobenia problémov. Sprievodca teda pokračuje na dodatkové nastavenia. V dodatkových nastaveniach je potrebné nastaviť NetBIOS doménové meno, ktoré je v tomto prípade nastavené na „test“.



Obrázok 58 : Nastavenie NetBIOS doménového mena (vlastný zdroj)

Po tomto nastavení následuje posledné nastavenie ciest pre uloženie AD DS databáz (to sú presne tie, ku ktorým je potrebné DSRM heslo). Tieto cesty sú preddefinované, takže ich nie je potrebné meniť, pokiaľ teda administrátor nechce, aby sa tieto databázy ukladali inam.

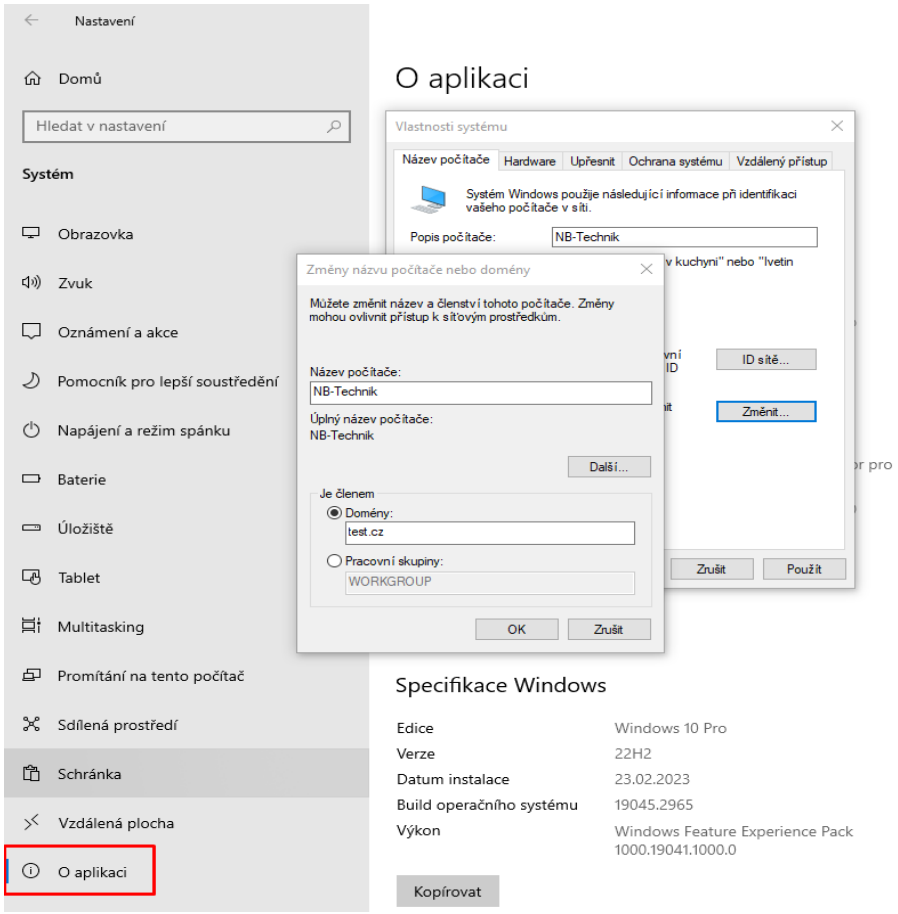


Obrázok 59 : Nastavenie ciest pre uloženie AD DS databáz (vlastný zdroj) C

Toto bolo finálne nastavenie, za ním nasleduje štandardne prehľad toho, čo bolo nastavované, potom prebehne inštalácia a následne sa vypíše výsledok inštalácie. Tieto kroky nie je potrebné dokumentovať, neobsahujú dôležité informácie (kontrola už prebehla a výsledok bola úspešná inštalácia role). Po každej konfigurácii sa odporúča doménový radič reštartovať, čo prebehne aj v tomto prípade.

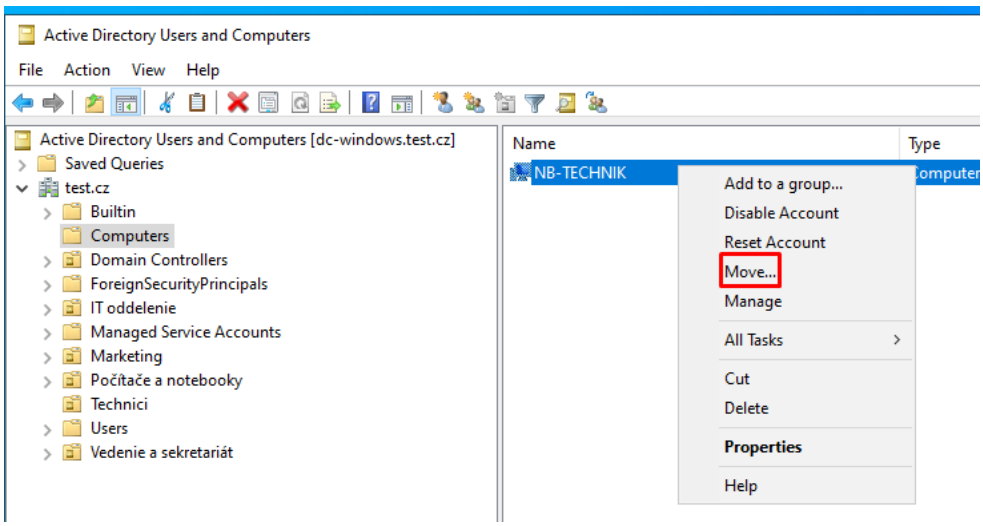
Po reštarte už počítač vystupuje ako doménový radič, konfigurácia bola úspešná, ďalej sa bude pokračovať konfiguráciou nainštalovaných rolí.

Teraz nasleduje krok testu – čiže pripojenie testovacieho zariadenia do domény. Tento krok sa realizuje v nastaveniach pod záložkami „O aplikaci“ a „Upřesnit nastavení systému“. Pre pripojenie zariadenia do domény je potrebné vedieť Administrátorské meno a heslo.



Obrázok 60 : Pripojenie počítača do domény (vlastný zdroj)

Po pripojení zariadenia do domény je potrebné toto zariadenie premiestniť z default OU „Computers“ do OU „Počítače a notebooky“.

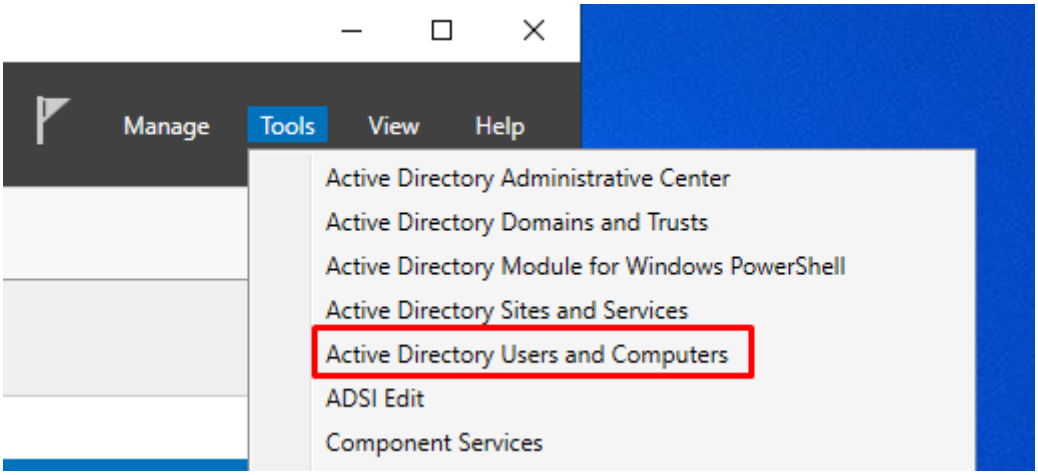


Obrázok 61 : Prvý krok premiestnenia zariadenia (vlastný zdroj)

5.3.2 AD DS – vytvorenie organizačných jednotiek, skupín, užívateľov a úložného priestoru pre užívateľov

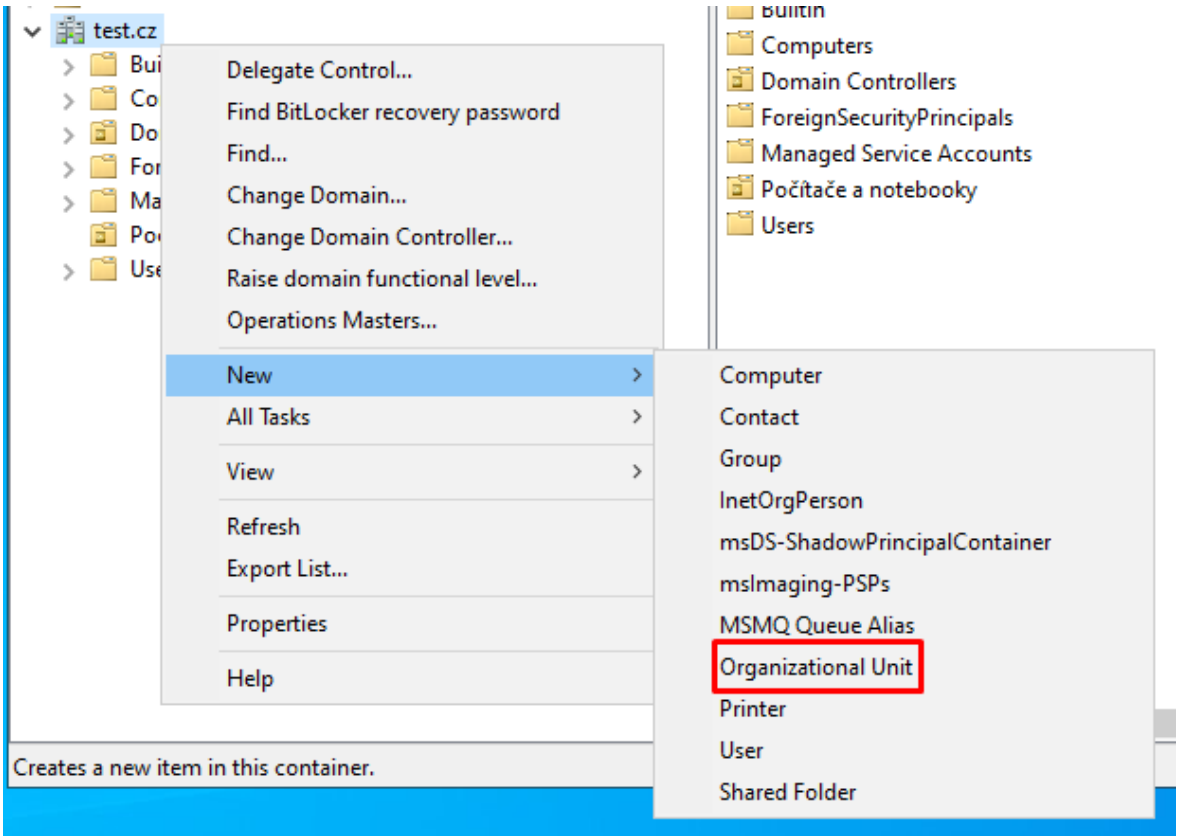
Rola AD DS bola úspešne nakonfigurovaná a z počítača sa stal doménový radič. AD DS je však potrebné naplniť vyššie zmienenými dátami, aby doménový radič mal pre koho a pre čo fungovať.

Začneme vytvorením organizačných jednotiek –v práci bude uvedená len jedna, keďže tie ostatné majú rovnakú konfiguráciu, len iný názov. Budú vytvorené nasledujúce organizačné jednotky – „Vedenie a sekretariát“, „IT“, „Technici“ a „Marketing“. Organizačné jednotky sa tvoria v „Active Directory Users and Computers“.



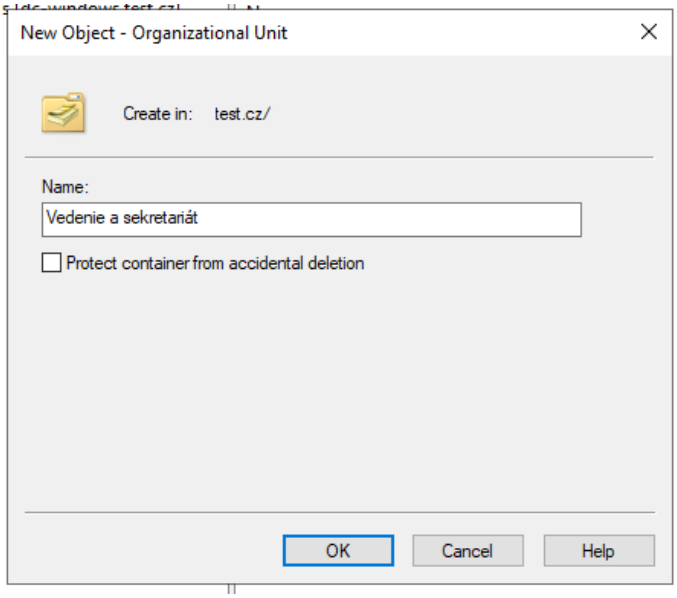
Obrázok 62 : Začiatok konfigurácie „Active Directory Users and Computer“ (vlastný zdroj)

Pre vytvorenie organizačných jednotiek je potrebné kliknúť pravým tlačidlom na „test.cz“ a v záložke vybrať možnosť „New“ a následne „Organizational Unit“.



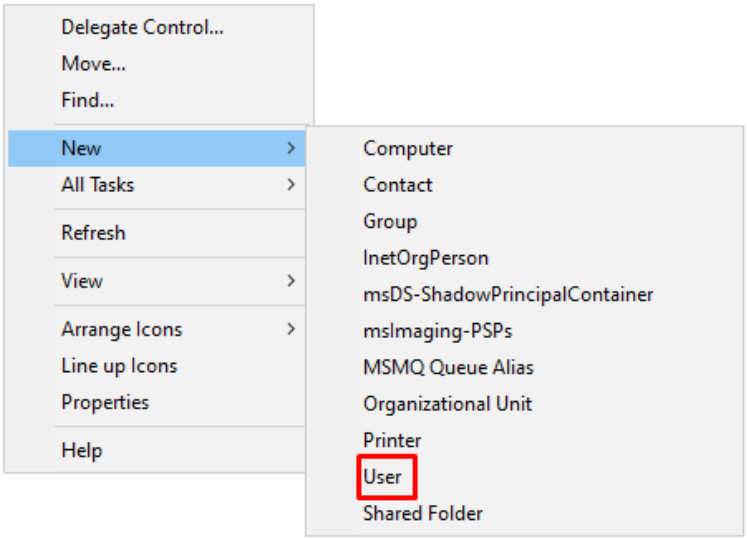
Obrázok 63 : Vytvorenie novej organizačnej jednotky (vlastný zdroj)

Následne je potrebné organizačnej jednotke nastaviť názov. Je tu checkbox s ponukou ochrany proti nechcenému zmazaniu – to bude odškrtnuté, pretože je potom postup odstránenia OU skomplikovaný ďalšími nastaveniami.



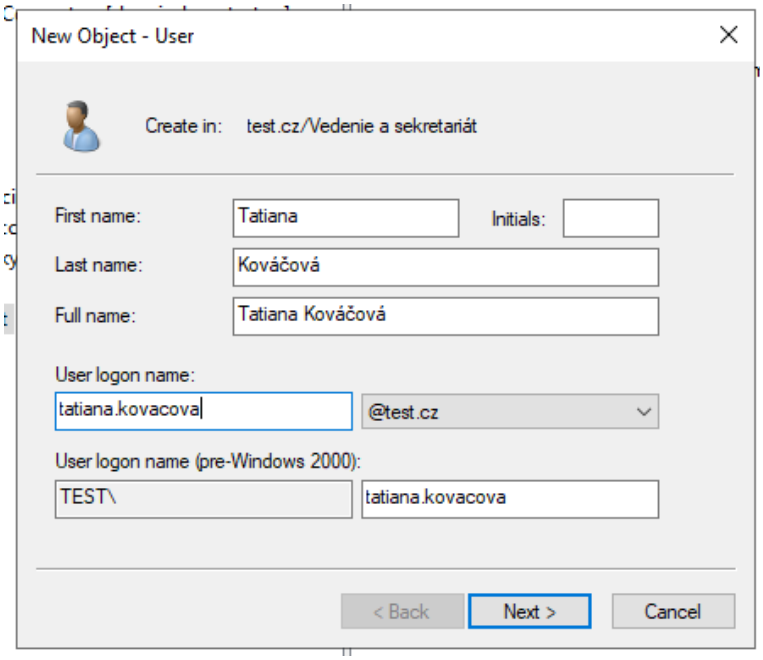
Obrázok 64 : Nastavenie názvu organizačnej jednotky (vlastný zdroj)

Týmto je organizačná jednotka vytvorená a teraz je do nej možné pridať / vytvoriť nových užívateľov. Stačí ju rozkliknúť, pravým tlačidlom kliknúť na ľubovoľné miesto a z možností si vybrať „New“ a „User“. Opäť v práci bude uvedené vytvorenie jedného užívateľa, ostatní sa vytvárajú rovnakým spôsobom, len sa im mení heslo pre prihlásenie.



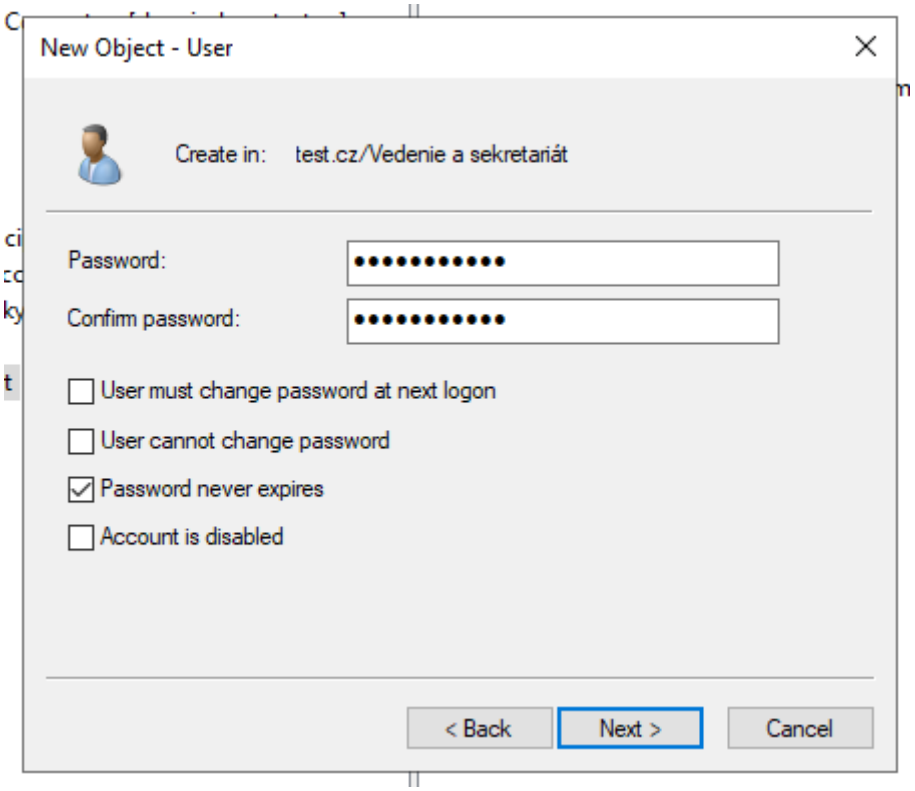
Obrázok 65 : Vytvorenie nového užívateľa (vlastný zdroj)

Pri vytváraní užívateľa je potrebné hneď na úvod vyplniť základné informácie, akými sú meno a login do domény.



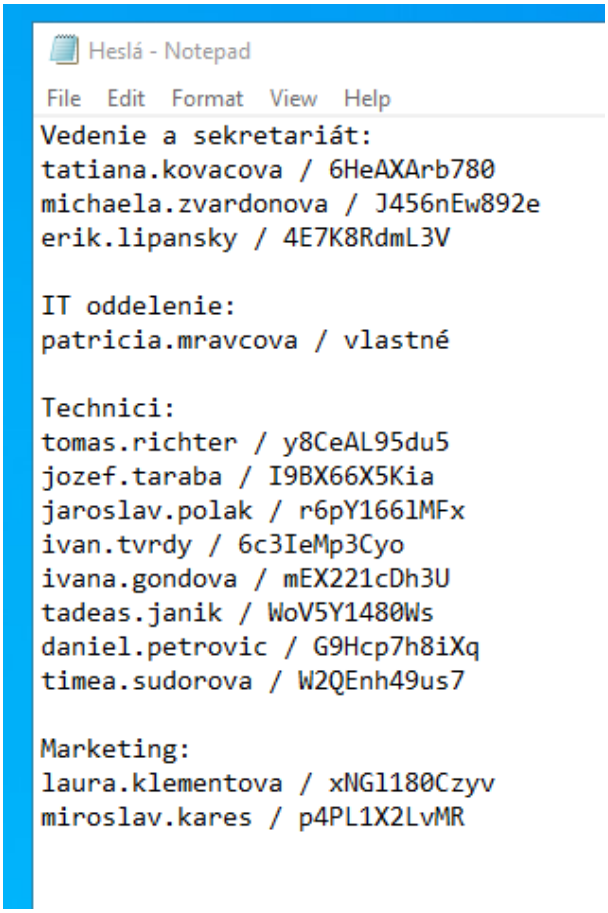
Obrázok 66 : Vyplnenie potrebných údajov užívateľa (vlastný zdroj)

Teraz je potrebné užívateľskému účtu nastaviť heslo a dodatočné parametre hesla (napríklad či si ho užívateľ môže meniť, či mu neskončí expirácia, či si užívateľ musí to heslo zmeniť pri ďalšom prihlásení atp.). Čo sa týka hesla pre užívateľa z administrátorského hľadiska nie je ideálne užívateľa donútiť používať vygenerované heslo a zároveň ani nie je ideálne nechať ho meniť si heslo bez restrikcií – všeobecne lepšou variantou je nastaviť random vygenerované heslo a následne si ho nechať užívateľa zmeniť, avšak požiadavky na heslo nastaviť pomocou skupinových politík.



Obrázok 67 : Nastavenie hesla pre užívateľa (vlastný zdroj)

Z praktických skúseností administrátora je lepšie si prvotné heslá niekam ukladať, pretože sa pomerne často stáva, že užívateľ heslo stratí ešte vôbec pred prvým prihlásením do zariadenia, aj keď to znie bizarne. V tejto testovacej štruktúre je vytvorených 15 užívateľov s random vygenerovanými heslami, ako je vidieť na obrázku nižšie. Tento textový súbor je však potrebné dobre uschovať – ideálne na samotnom radiči niekam, kam užívatelia prístup nemajú.



Obrázok 68 : Preventívne ukladanie hesiel (vlastný zdroj)

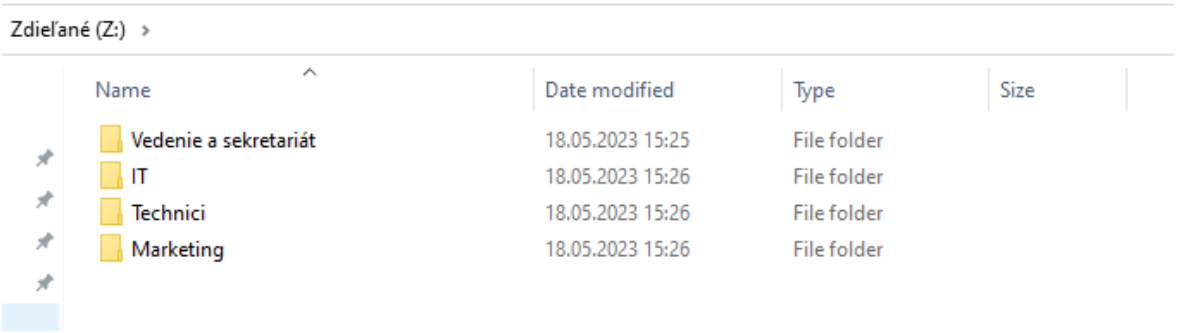
Vytvorenie zdieľaného zväzku:

Ďalším krokom bude vytvoriť úložný priestor, v ktorom sa budú nachádzať firemné zdieľané zložky– teda „Vedenie a sekretariát“, „IT“, „Technici“ a „Marketing“.

Začne sa teda tým, že bude potrebné vytvoriť nový zväzok, ako to bolo v prípade inštalácie role WSUS. Keďže tento krok už bol zdokumentovaný v kapitole 5.3 pod inštaláciou role WSUS, nebude táto časť znova dokumentovaná. Zvolí sa rovnaká kapacita, ako to bolo v prípade role WSUS – teda 100 GB. Nový zväzok bude pomenovaný „Z:“ ako zdieľané.

V týchto zložkách sa budú nachádzať firemné dokumenty, potrebné pre prácu jednotlivých oddelení. Následne sa vytvoria v organizačných jednotkách špeciálne skupiny, pomocou ktorých sa bude prístup k týmto firemným zdrojom delegovať.

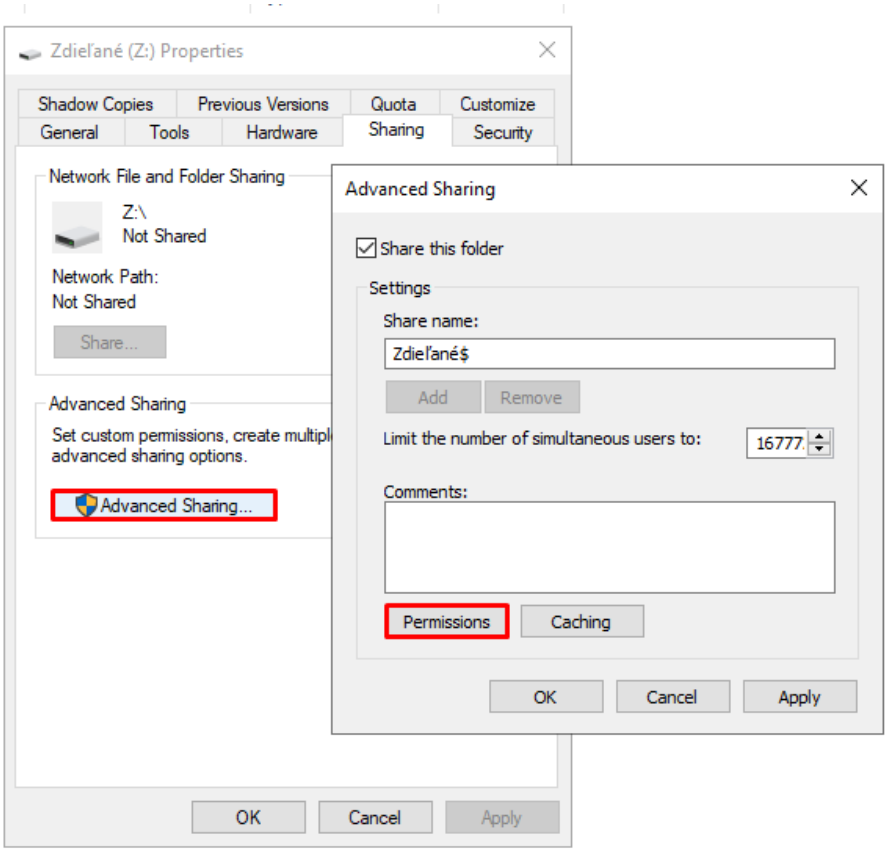
Po vytvorení tohto zväzku je potrebné ho nastaviť ako zdieľaný zväzok pre skupinu „Users“, kam spadajú všetci užívatelia.



Obrázok 69 : Vytvorenie zložiek (vlastný zdroj)

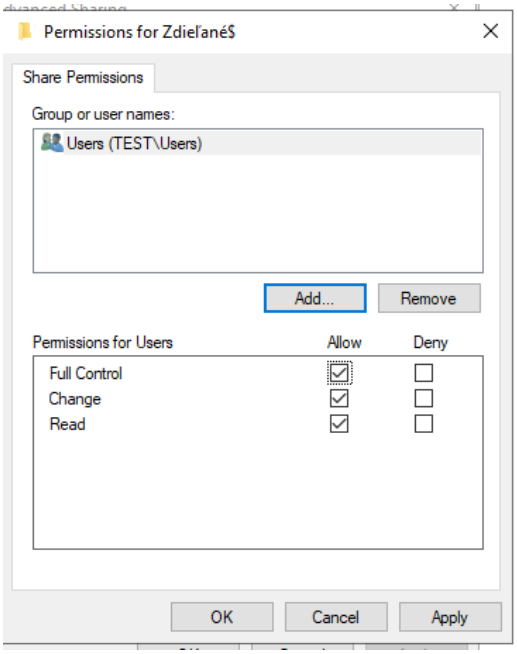
Obrázok 70 : Vlastnosti zdieľaného disku (vlastný zdroj)

Vo vlastnostiach disku je potrebné pod záložkou „Sharing“ nájsť možnosť „Advanced Sharing“, kde je potrebné nastaviť názov (v tomto prípade „Zdieľané$“ – znak „$“ zabezpečuje, že zložka nie je viditeľná) a zároveň povolenia, s kým môže byť zväzok zdieľaný. Nastavená bola skupina „Users“, kam patria všetci užívatelia – je to zdieľaný pracovný zväzok pre všetkých.



Obrázok 71 : Nastavenie názvu a povolení (vlastný zdroj)

Ďalšie kroky potom smerujú ku delegácii prístupu pomocou bezpečnostných skupín, ktoré rieši iná časť diplomovej práce.

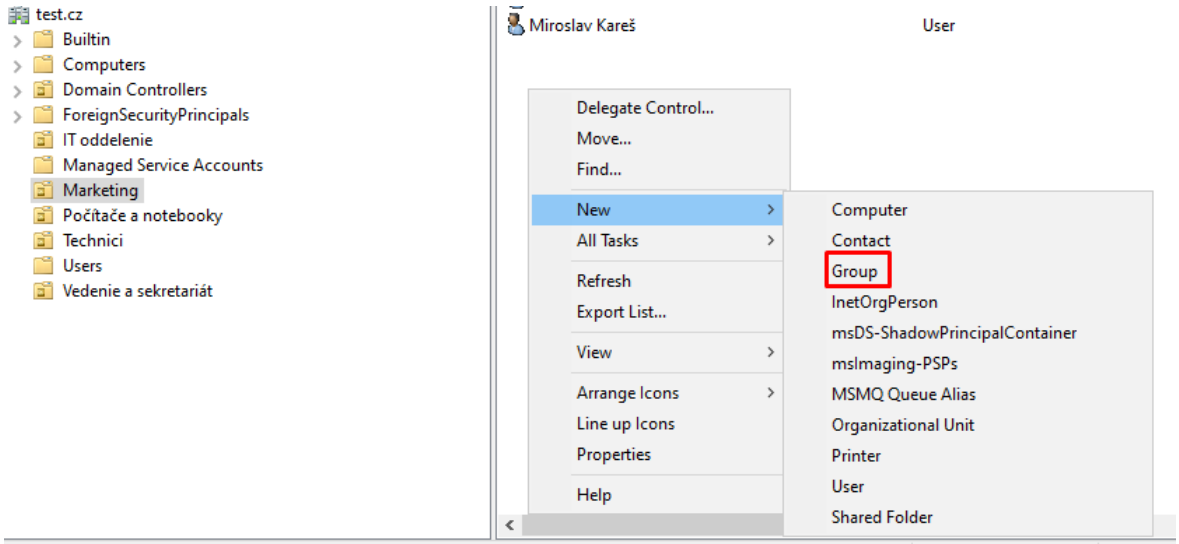


Obrázok 72 : Nastavenie povolenia prístupu pre „Users“ (vlastný zdroj)

Teraz je potrebné presunúť sa ku kroku vytvorenia skupín – skupiny sa zatiaľ len vytvoria, ich nastavenie potom rozoberá iná časť diplomovej práce.

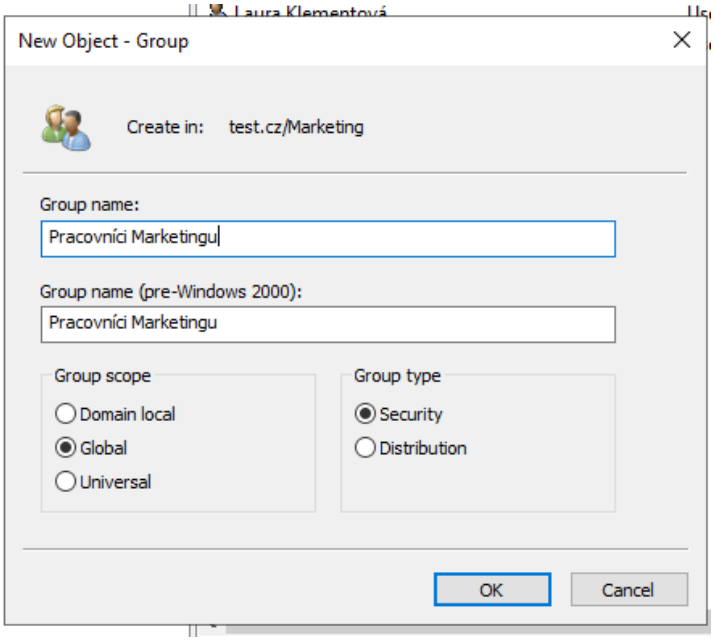
Tak, ako to bolo v predošlých častiach, zdokumentované bude vytvorenie len jednej skupiny a tou je „Pracovníci Marketingu“, ostatné skupiny sa nastavujú úplne rovnakým spôsobom, len majú iný názov. Ďalšími skupinami budú: „Vedenie“, „Sekretári“, „Účtovníci“, „Pracovníci vedenia a sekretariátu“, „Pracovníci IT oddelenia“, „Pracovníci technického oddelenia“, „Projektanti“, „Údržbári“, „Elektrikári“ a „Stavbári“.

Skupiny sa vytvárajú v „Active Directory Users and Computers“, stačí prejsť na zvolenú organizačnú jednotku, kliknúť pravým tlačidlom, zvoliť možnosti „New“ a „Group“.



Obrázok 73 : Vytvorenie novej skupiny (vlastný zdroj)

Pri vytvorení skupiny je potrebné nastaviť jej názov, dosah a typ. Názvom teda bude „Pracovníci Marketingu“, dosah bude globálny (bude sa teda týkať celej siete) a čo sa týka typu skupiny, tak bude bezpečnostná.



Obrázok 74 : Nastavenie parametrov skupiny (vlastný zdroj)

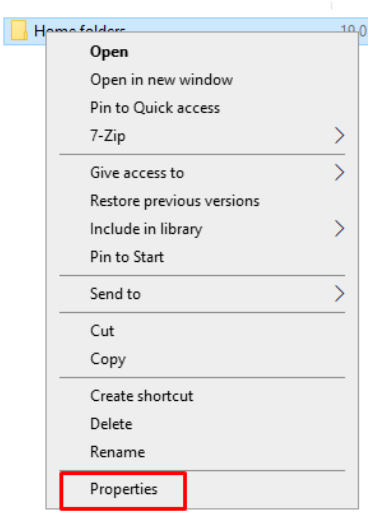
Po tomto kroku je do skupín potrebné zaradiť členov podľa potreby, pre praktickú časť diplomovej práce sú užívatelia rozdelení náhodne.

Vytvorenie Home Folders:

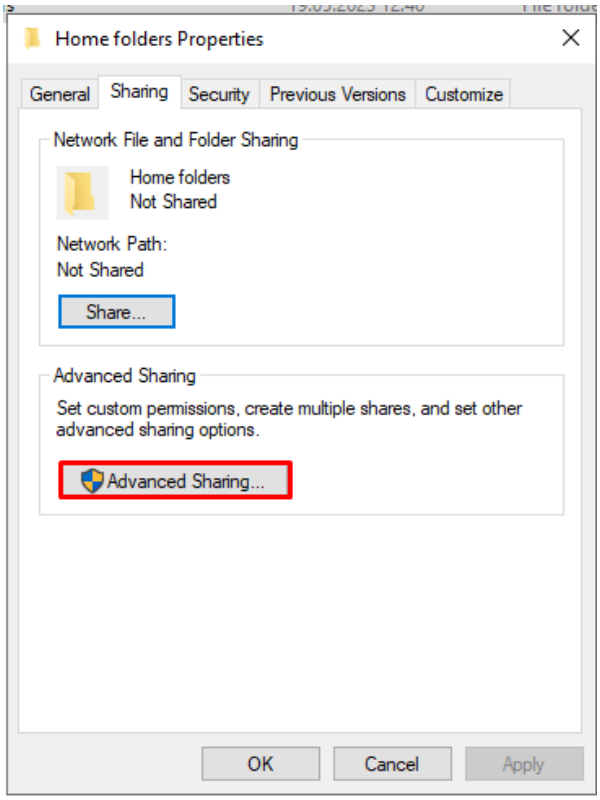
Posledným krokom je nastaviť pre užívateľov úložisko- súkromnú zložku priamo v úložisku radiča, kde si budú môcť ukladať a zálohovať. Toto nastavenie chráni administrátora a zamestnanca v tom smere, že pokiaľ zariadenie bude odcudzené, prípadne vypovedá službu, užívateľ nájde svoje dáta bez ohľadu na zariadenie. Či už si ich tam však bude zálohovať je na ňom, každopádne potom nemôže prísť za vedením a sťažovať si na stratené dáta.

Začne sa teda tým, že bude potrebné vytvoriť nový zväzok, ako to bolo v prípade inštalácie role WSUS. Keďže tento krok už bol zdokumentovaný v kapitole 5.3 pod inštaláciou role WSUS, nebude táto časť znova dokumentovaná. Zvolí sa rovnaká kapacita, ako to bolo v prípade role WSUS – teda 100 GB. Zväzok bude pomenovaný „O:“ ako osobné.

Na novo vytvorenom zväzku sa vytvorí zložka „Home Folders“ – v túto zložku je zároveň potrebné nastaviť ako zdieľanú zložku. Toto nastavenie sa nachádza vo vlastnostiach, konkrétne v záložke „Sharing“.

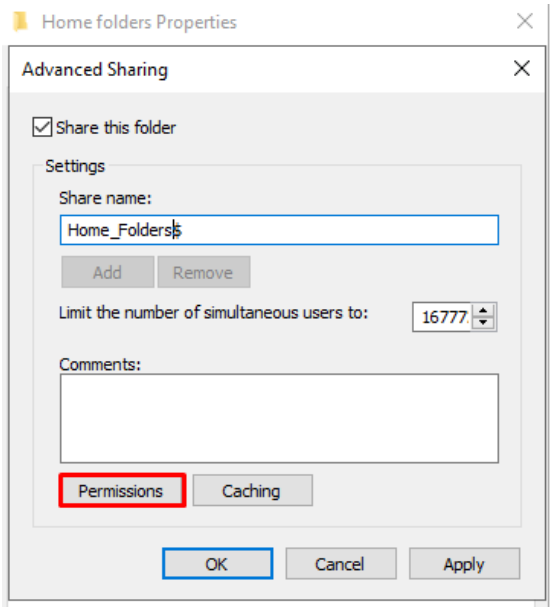


Obrázok 75 : Nastavenie parametrov skupiny (vlastný zdroj)

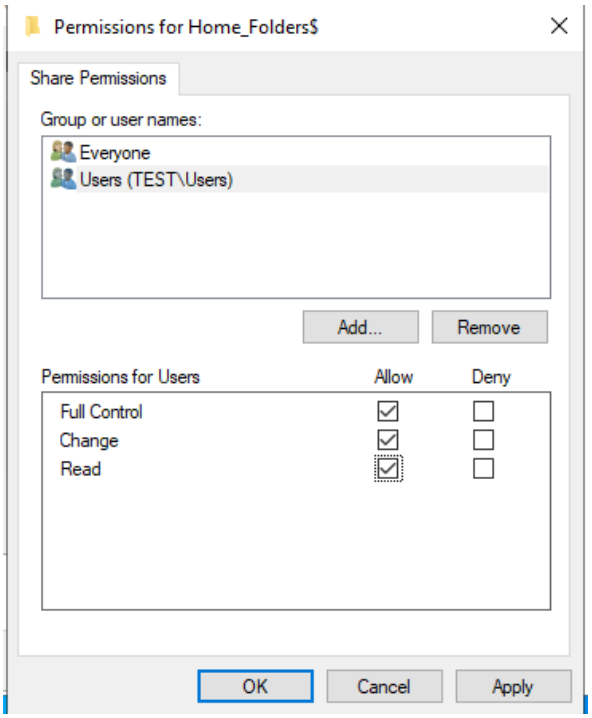


Obrázok 76 : Nastavenie parametrov skupiny (vlastný zdroj)

Ďalej je potrebné nastaviť názov zdieľanej zložky a špecifikovať skupiny, ktoré majú mať k nej prístup. Zvolená bola default skupina „Users“, ktorú dostane každý novo vytvorený užívateľ automaticky.

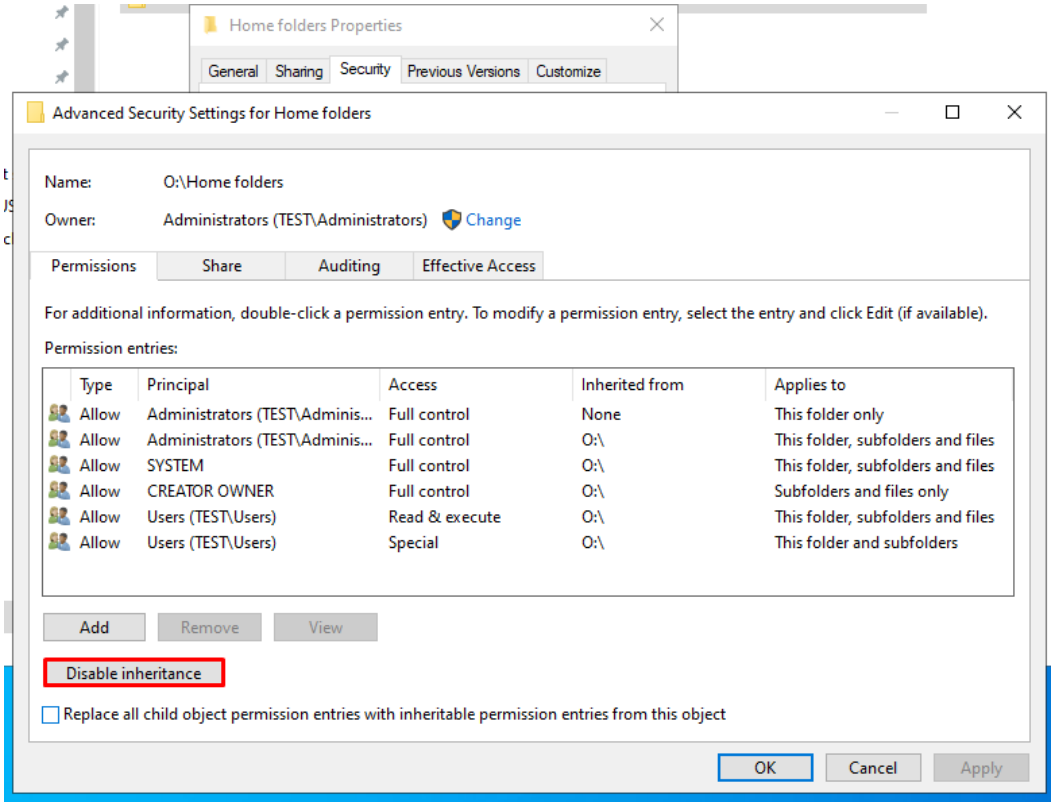


Obrázok 77 : Nastavenie názvu (vlastný zdroj)



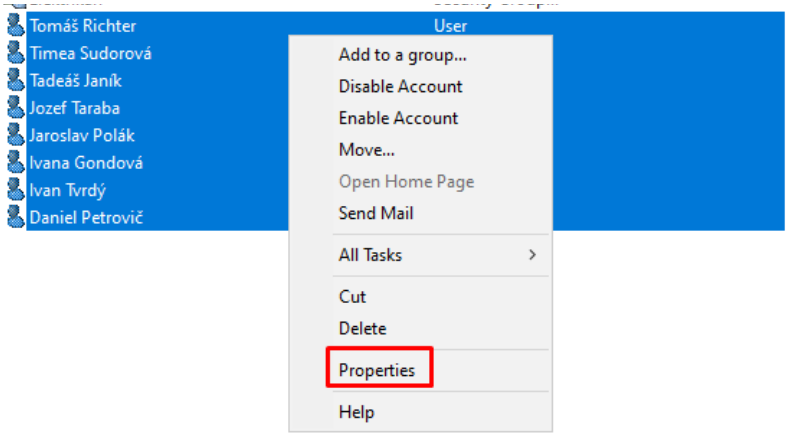
Obrázok 78 : Nastavenie skupín s povoleným prístupom (vlastný zdroj)

Ďalším krokom je zakázanie dedenia a zmazanie nepotrebných skupín z povolení (teda aby zložku mohol editovať len administrátor).



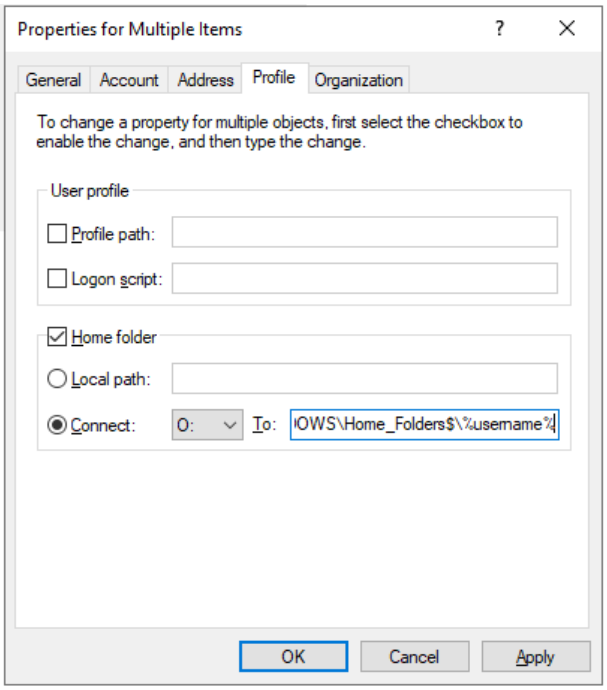
Obrázok 79 : Zakázanie dedenia zmazanie nepotrebných skupín (vlastný zdroj)

V tejto chvíli je potrebné namapovať domovské adresáre užívateľom, toto je potrebné nastaviť v ADUC.



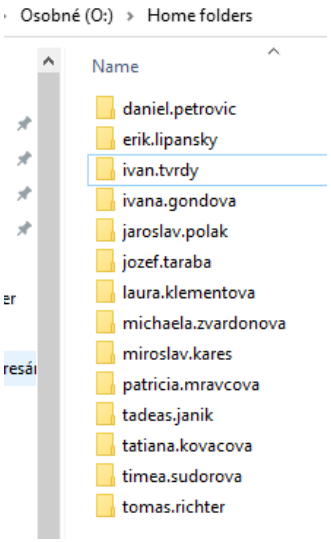
Obrázok 80 : Začiatok vytvorenia home folders pre viacerých užívateľov (vlastný zdroj)

V ďalšom kroku je potrebné definovať, cestu k úložisku, a za neho vložiť ešte jedno spätné lomítko s pamametrom „%username%“, ktorý sa postará o to, aby sa vytvorila zložka pre užívateľa s jeho vlastným menom.



Obrázok 81 : Namapovanie zložiek pre užívateľov (vlastný zdroj)

Teraz je potrebné si overiť, či nastavenie funguje tak, ako má. Funguje, zložky v „Home Folders“ sa úspešne vytvorili.

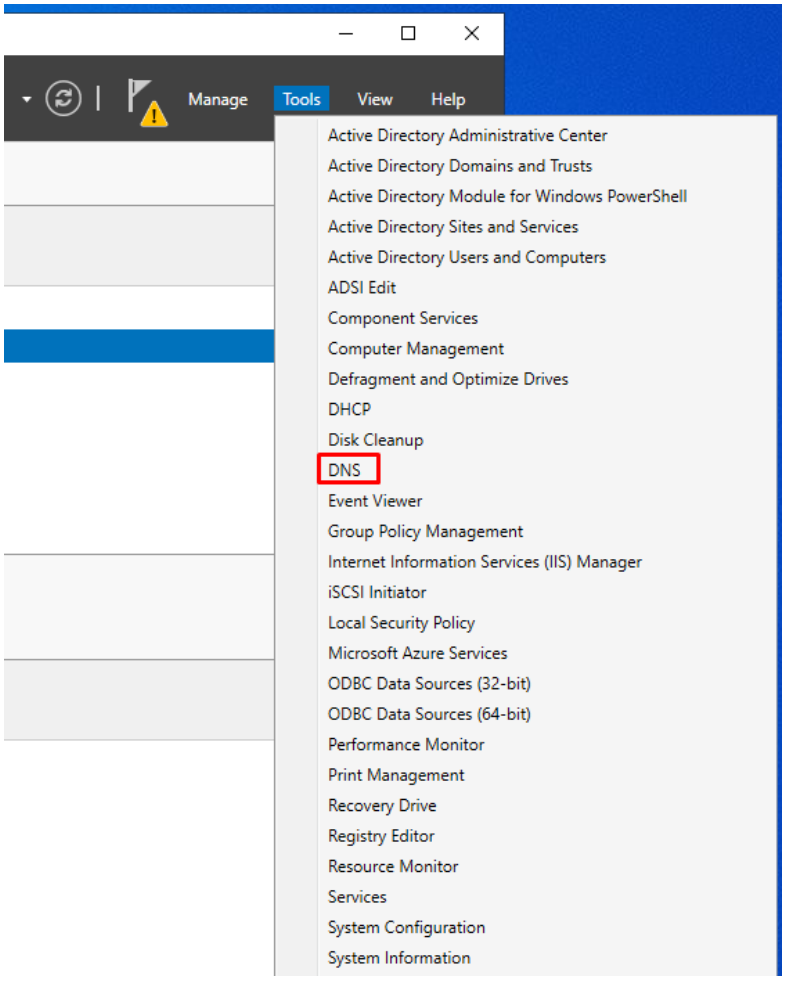


Obrázok 82 : Úspešne vytvorené zložky (vlastný zdroj)

5.3.3 Konfigurácia role DNS

Táto rola bude vykonávať pre radič funkciu dopredného a reverzného prekladu. Ako bolo uvedené v teoretickej časti, DNS poskytuje veľké množstvo záznamov, pričom každý má inú funkciu. Je potrebné, aby jednou z funkcií tohto doménového radiča bolo poskytovať dopredný a reverzný preklad, aby túto funkciu nezastupoval router, prípadne servery spoločnosti google. Základnou konfiguráciou role DNS sa dosiahne to, že preklad prebieha vnútri siete, pričom je za neho zodpovedný radič. Toto nastavenie sa hodí napríklad pre tlačiareň – z bezpečnostného hľadiska nie je vhodné, aby tlačiareň pre komunikáciu v sieti využívala DNS servery spoločnosti, ktorá ju vyrába (samozrejme možné to je, ale z bezpečnostného hľadiska to nie je ideálne riešenie).

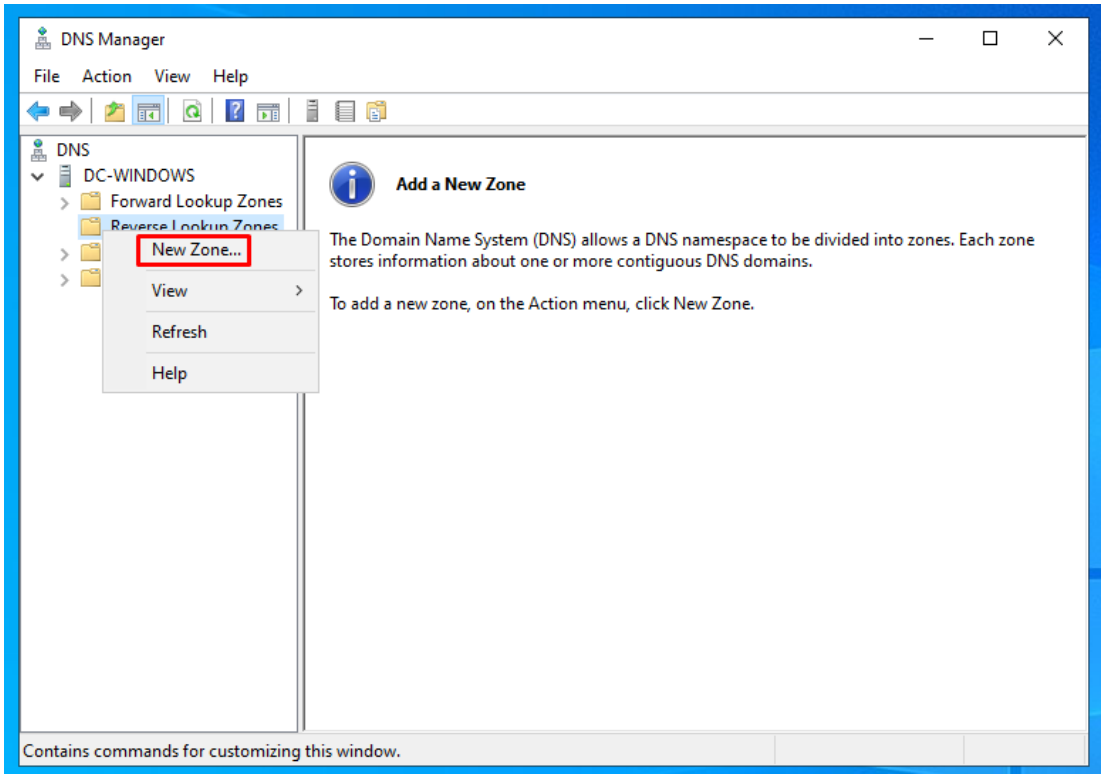
V hornej lište server manageru sa nachádza políčko „Tools“, ktoré po rozkliknutí zobrazí všetky role a súčasti, ktoré je možné v danej chvíli konfigurovať. Vybraná teda bude možnosť „DNS“.



Obrázok 83 : Začiatok konfigurácie role DNS (vlastný zdroj)

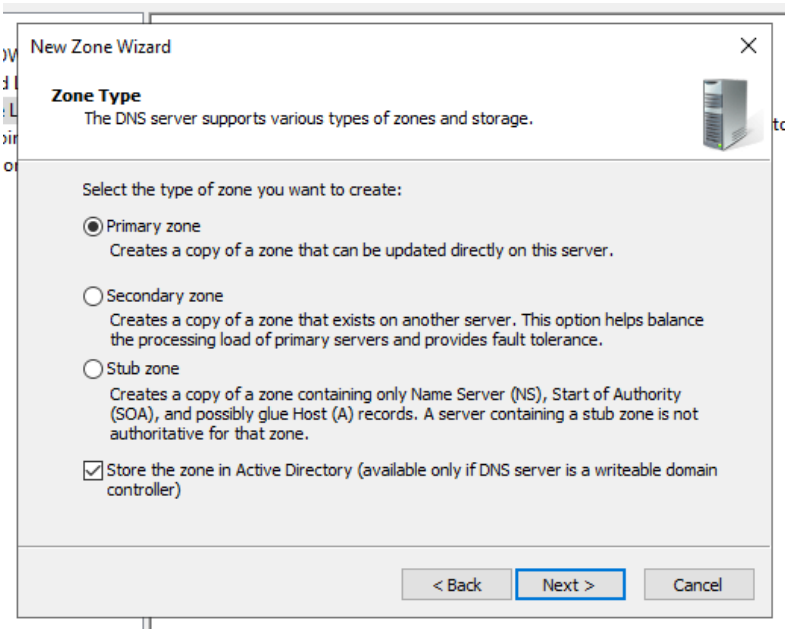
Následne sa tvorí DNS manager, kde je možné rolu DNS konfigurovať, takže sa môže pokračovať s konfiguráciou forward a reverse zón.

Začne sa konfiguráciou reverse zóny, ktorá je jednoduchšia. Stačí kliknúť na zložku „Reverse Lookup Zones“ pravým tlačidlom a vybrať možnosť „New Zone...“



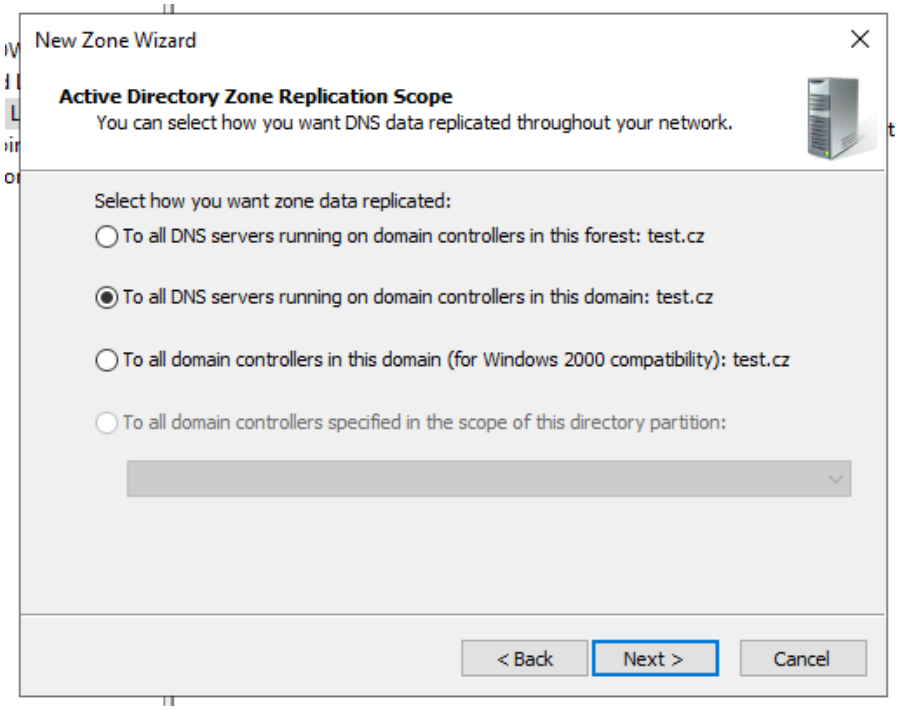
Obrázok 84 : Vytvorenie novej reverse zóny (vlastný zdroj)

Klasicky sa zobrazí sprievodca konfiguráciou. Ako typ zóny bude vybraná primárna zóna.



Obrázok 85 : Výber typu zóny (vlastný zdroj)

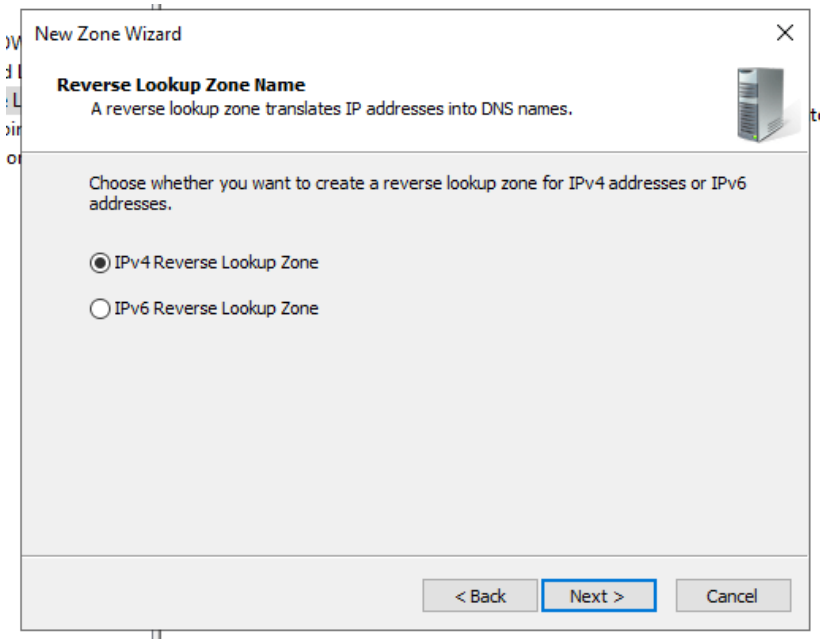
Nasleduje výber spôsobu replikácie dát, vybraná bude druhá možnosť.



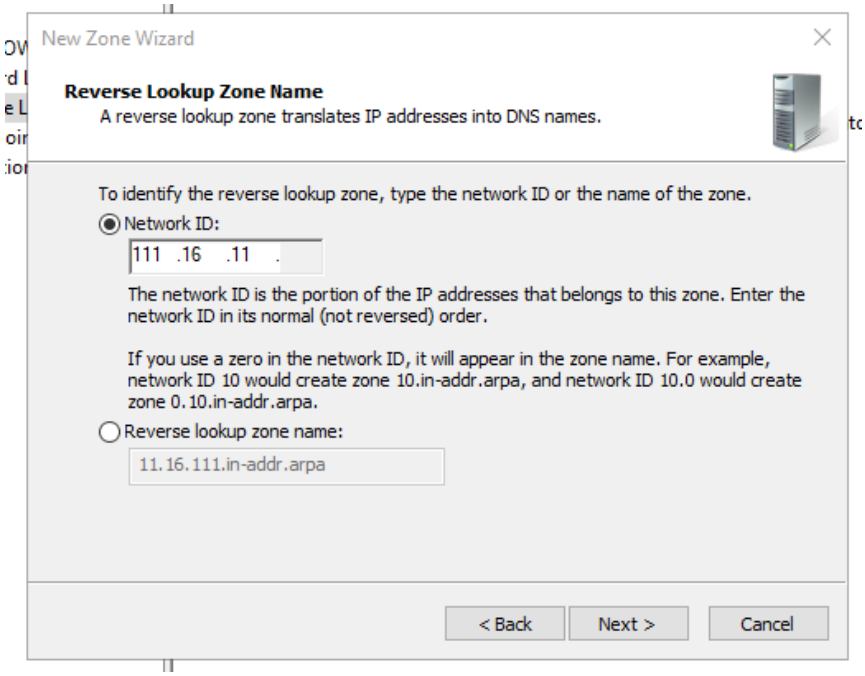
Obrázok 86 : Výber spôsobu replikácie dát (vlastný zdroj)

Po tomto kroku nasleduje výber protokolu, buď bude preklad prebiehať pre IPv4, alebo IPv6. Vybraná bude možnosť s IPv4.

Následne je potrebné vyplniť „Network ID“, so sú v podstate prvé tri oktety IP adresy siete.

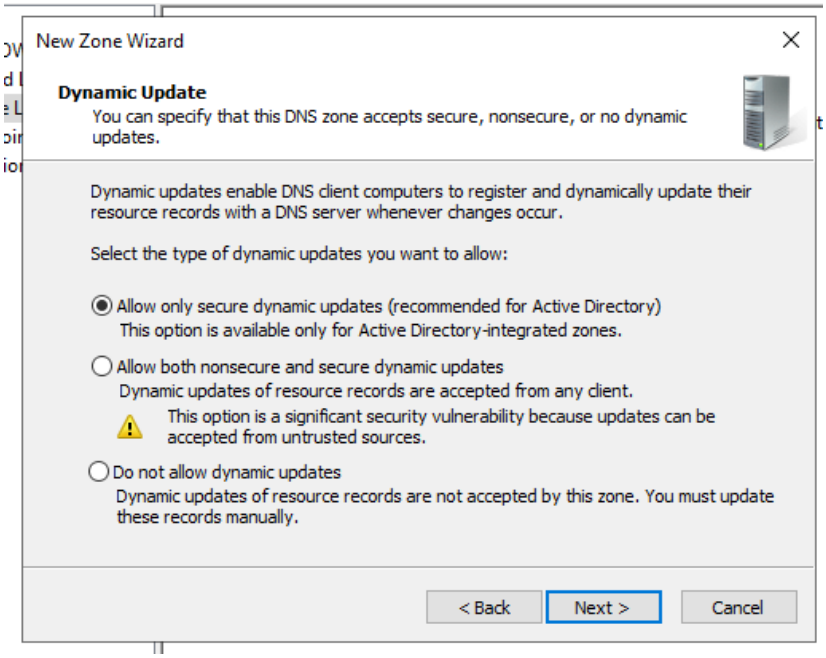


Obrázok 87 : Výber spôsobu replikácie dát (vlastný zdroj)



Obrázok 88 : Vyplnenie Network ID (vlastný zdroj)

Ďalší krok sa zaoberá výberom aktualizácií – bude vybraná odporúčaná možnosť.

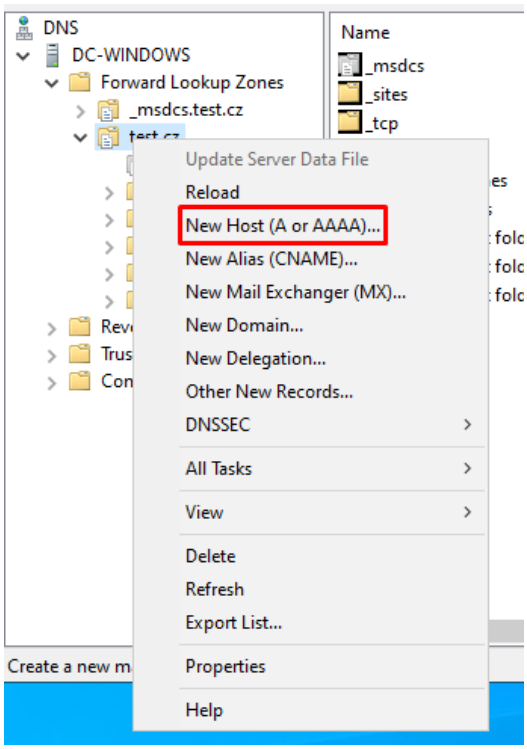


Obrázok 89 : Výber typu aktualizácií (vlastný zdroj)

Toto bol posledný krok, ktorý bolo potrebné vyplniť, stačí výber už len potvrdiť v sprievodcovi a reverse zóna je vytvorená.

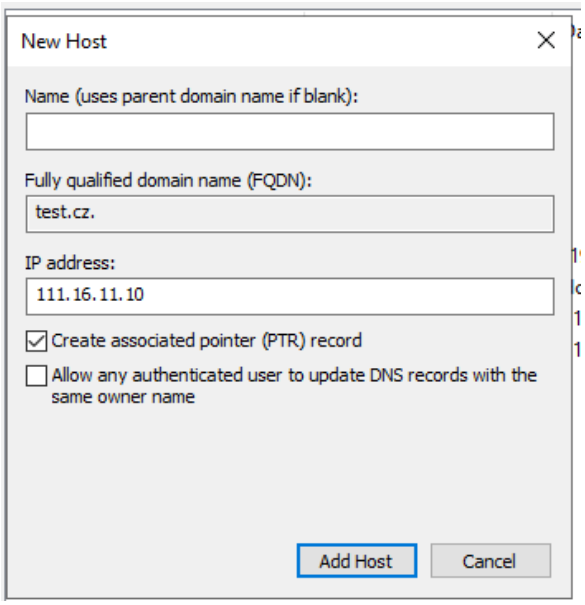
Teraz je ešte potrebné nastaviť forward zónu, kde už nastavenie neprebieha podľa sprievodcu, ale vkladajú sa konkrétne typy záznamov podľa potreby.

Prvým záznamom, ktorý je potrebné nastaviť je záznam A, ktorý slúži pre nasmerovanie domény na konkrétnu IP adresu. Ako IP adresa sa nastavuje IP adresa doménového radiča.



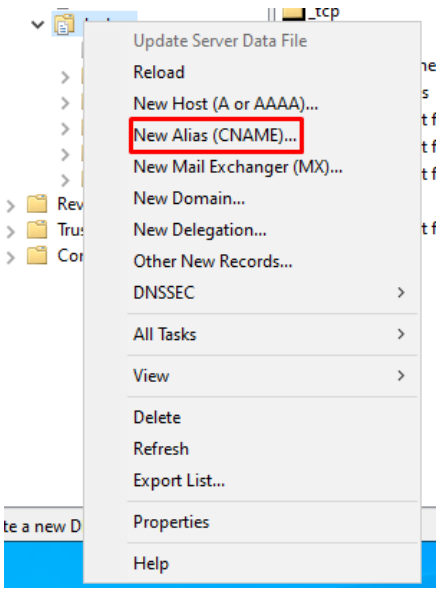
Obrázok 90 : Pridanie A záznamu (vlastný zdroj)

Ešte je potrebné zaškrtnúť možnosť „Create associated pointer record“ čo je v podstate reverzný záznam.



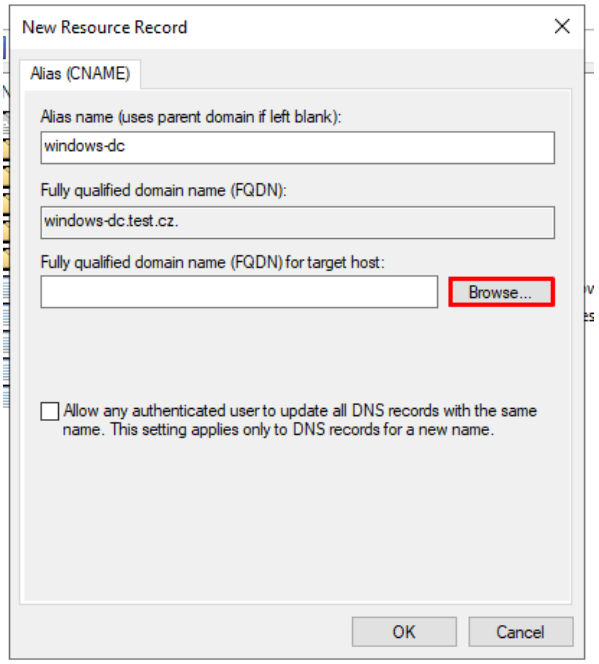
Obrázok 91 : Nastavenie A záznamu (vlastný zdroj)

V tejto chvíli je dopredné a spätné vyhľadávanie nastavené, ešte pre príklad sa nastaví záznam CNAME. To je záznam, ktorý slúži na nasmerovanie (napríklad na inú doménu). Bude nakonfigurovaný tak, aby sa dalo k doménovému radiču pripojiť nielen zadaním názvu „dc-windows.test.cz“, ale aj zadaním názvu „windows-dc.test.cz“.



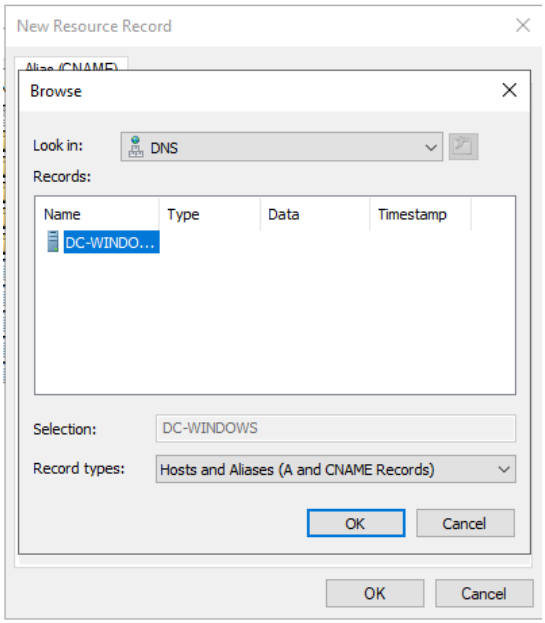
Obrázok 92 : Pridanie CNAME záznamu (vlastný zdroj)

Najprv sa teda vyberie názov aliasu a následne je potrebné nastaviť FQDN pre cieľového hosta.

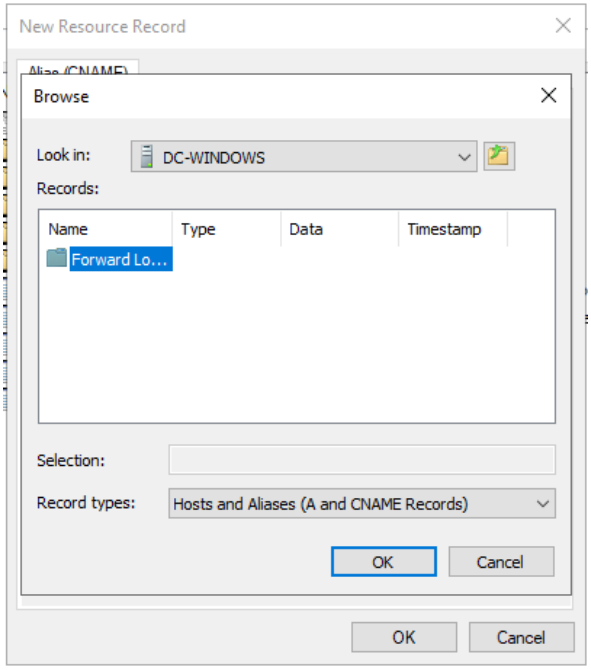


Obrázok 93 : Nastavenie CNAME záznamu (vlastný zdroj)

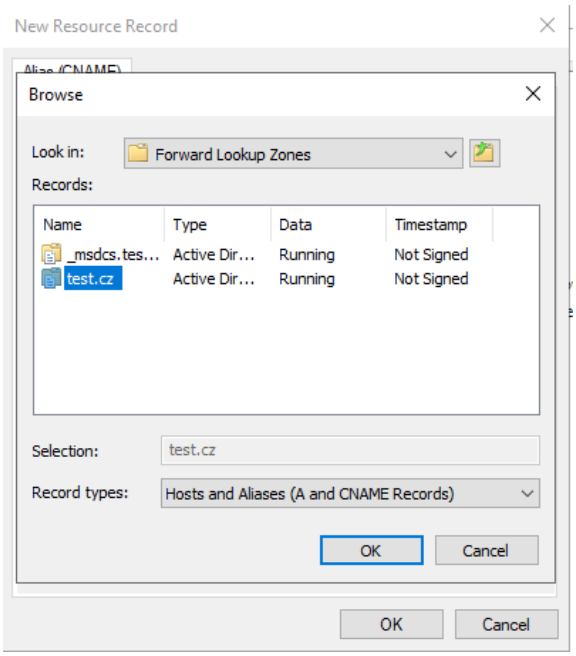
Pri zadaní možnosti „browse“ sa zobrazí sprievodca, ktorý sa z veľkej časti len prekliká.



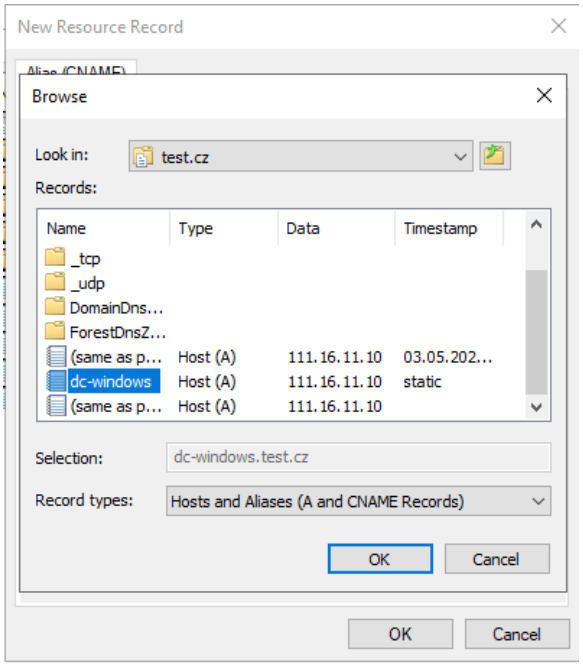
Obrázok 94 : Výber DNS serveru (vlastný zdroj)



Obrázok 95 : Výber forward zóny (vlastný zdroj)

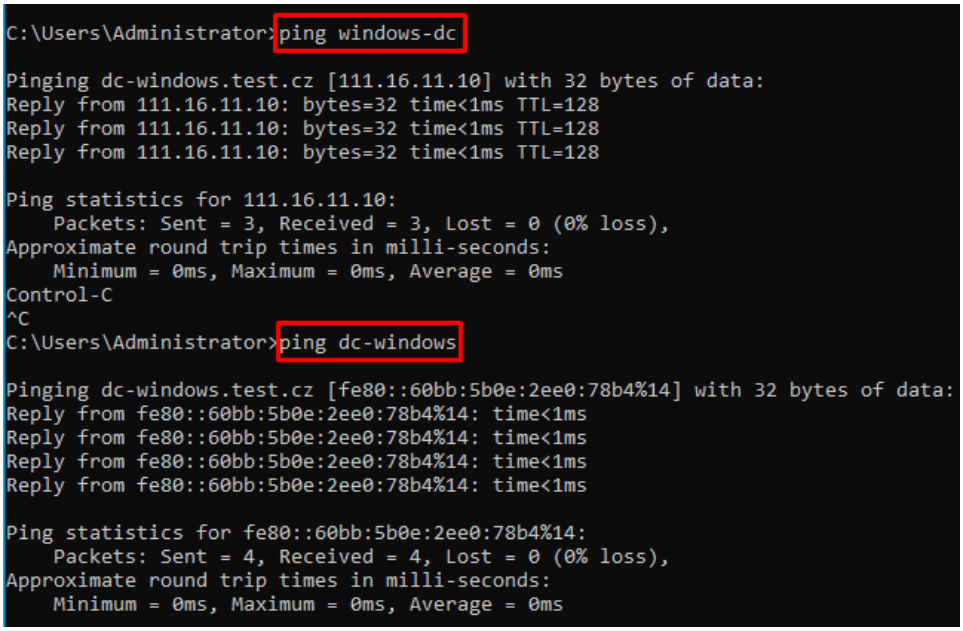


Obrázok 96 : Výber forward zóny test.cz (vlastný zdroj)



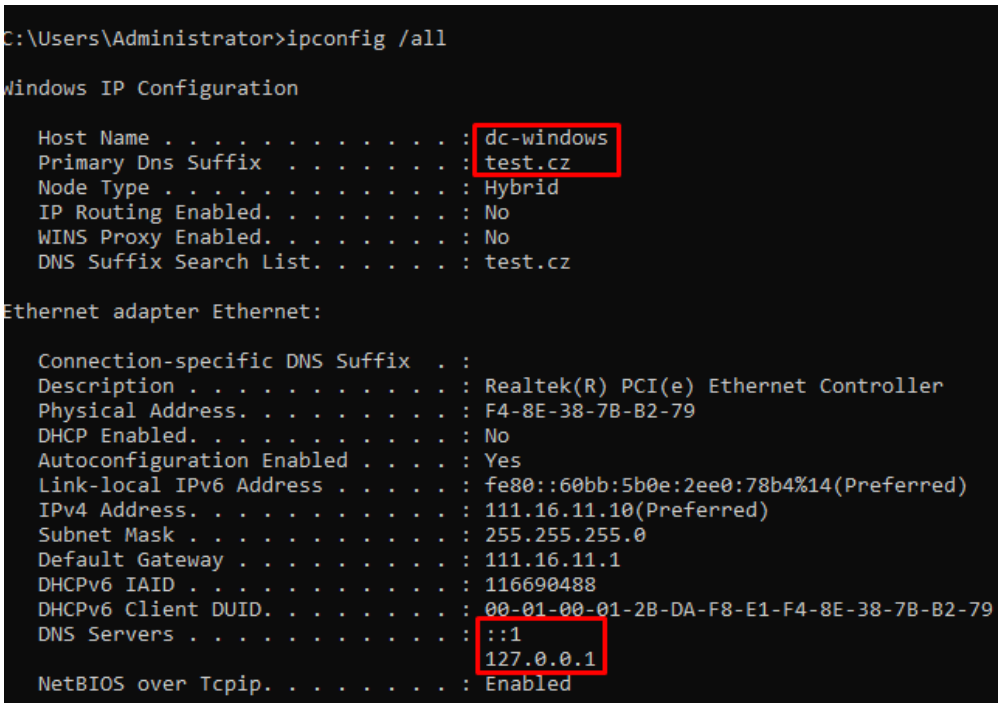
Obrázok 97 : Výber target hosta (vlastný zdroj)

Týmto je sprievodca dokončený a CNAME záznam nakonfigurovaný. Ostáva už len otestovať jeho funkčnosť.



Obrázok 98 : Ping test CNAME (vlastný zdroj)

Ako je vidieť na obrázku vyššie, ping funguje na obe hostnames, čiže CNAME záznam je nastavený správne. Ešte ostáva overiť si funkčnosť DNS.



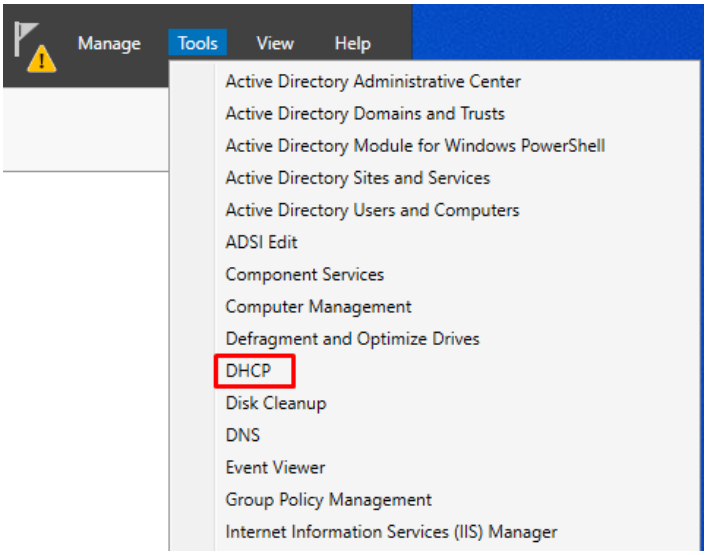
Obrázok 99 : Test DNS (vlastný zdroj)

Týmto je dokončená konfigurácia role DNS.

5.3.4 Konfigurácia role DHCP

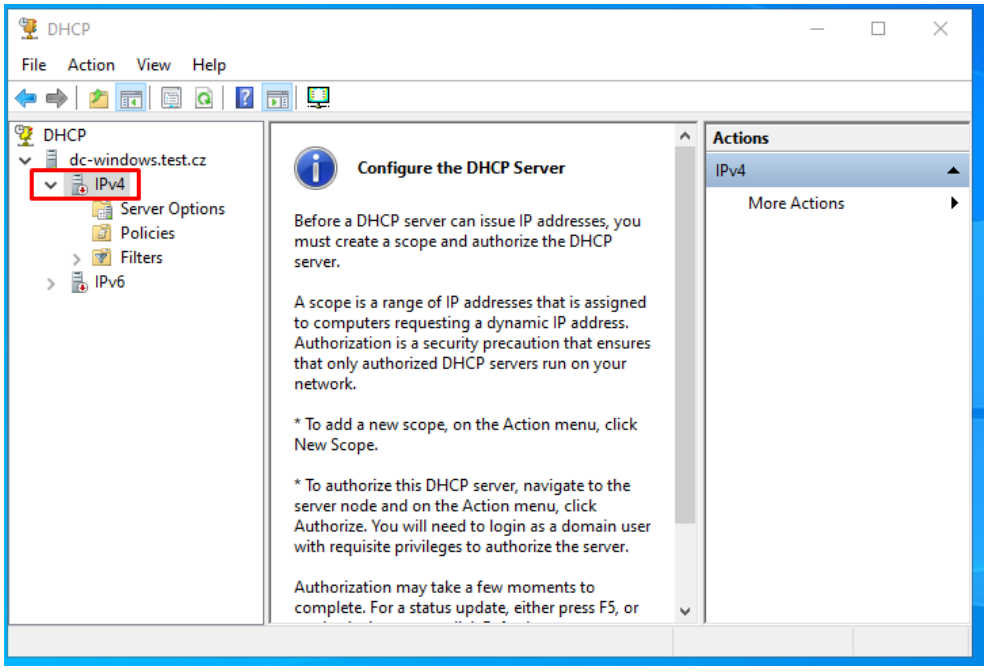
Táto rola je dôležitá pre poskytovanie sieťových informácií jednotlivým zariadeniam v sieti.

Konfigurácia tejto role začína rovnako, ako konfigurácia role DNS, po kliknutí na „Tools“.

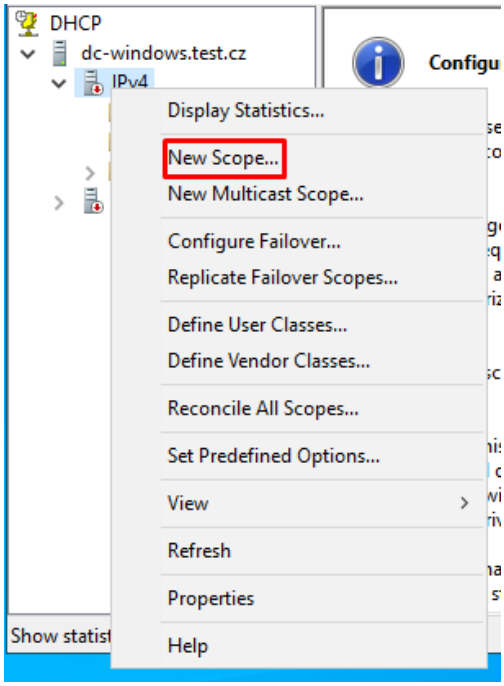


Obrázok 100 : Začiatok konfigurácie role DHCP (vlastný zdroj),

Po rozkliknutí sa otvorí DHCP manager, kde je možné rolu DHCP konfigurovať pre IPv4 a IPv6. Vybraná bude konfigurácia pre IPv4, kde sa na ikonku klikne pravým tlačidlom a vyberie sa možnosť „New Scope...“.

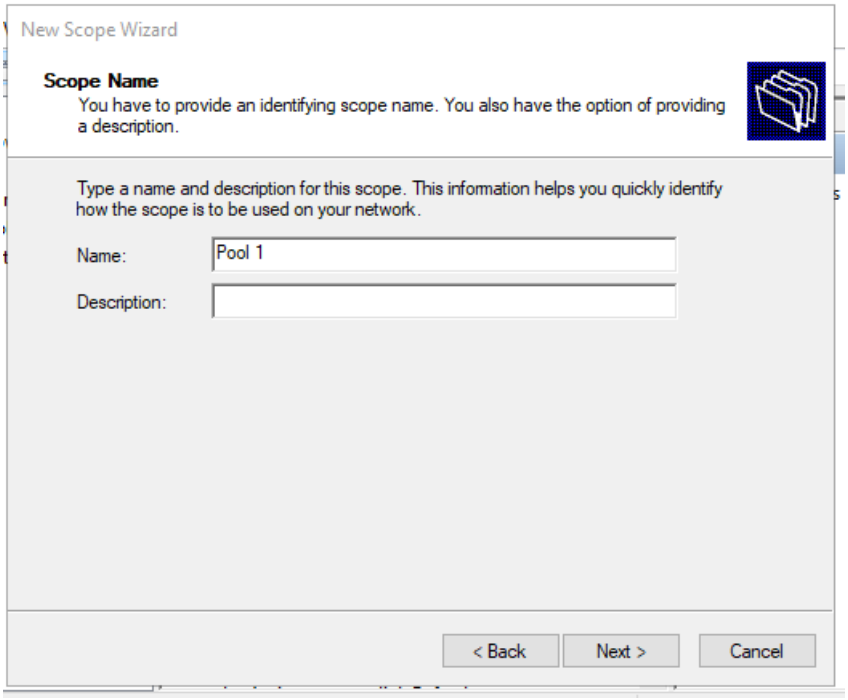


Obrázok 101 :Začiatok konfigurácie role DHCP (vlastný zdroj)



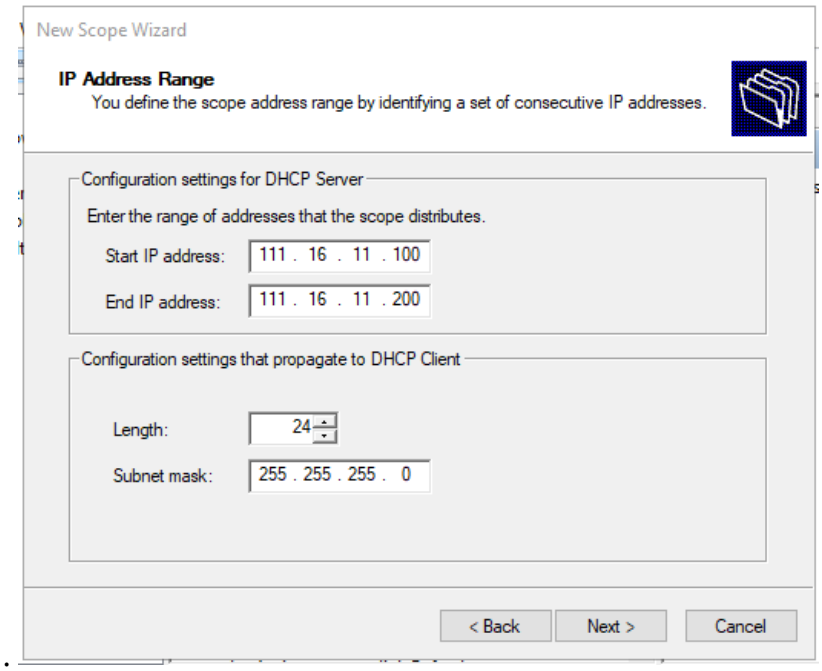
Obrázok 102 :Vytvorenie nového rozsahu pre IPv4 (vlastný zdroj)

Týmto sa začne konfigurácia nového rozsahu s využitím IP adries typu IPv4. Najprv je potrebné zadať názov rozsahu, vybraný názov je „Pool 1“.



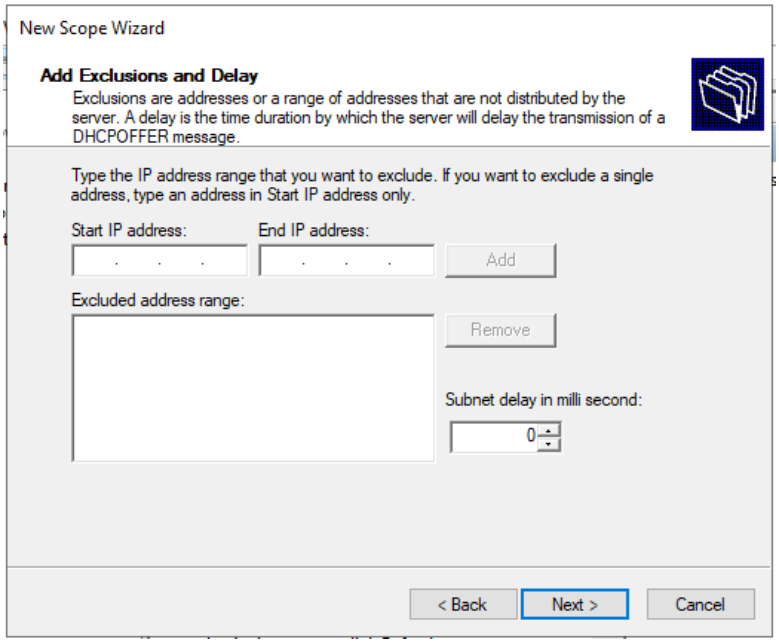
Obrázok 103 : Zadanie názvu rozsahu (vlastný zdroj)

Následne je potrebné nastaviť samotný rozsah – čiže rozsah adries, ktoré sa budú prideľovať zariadeniam. Pre lepšiu zapamätateľnosť bol vybraný rozsah od 100 – 200, ešte je potrebné nastaviť masku, v tomto prípade je prefix /24, ku ktorému prislúcha maska 255.255.255.0



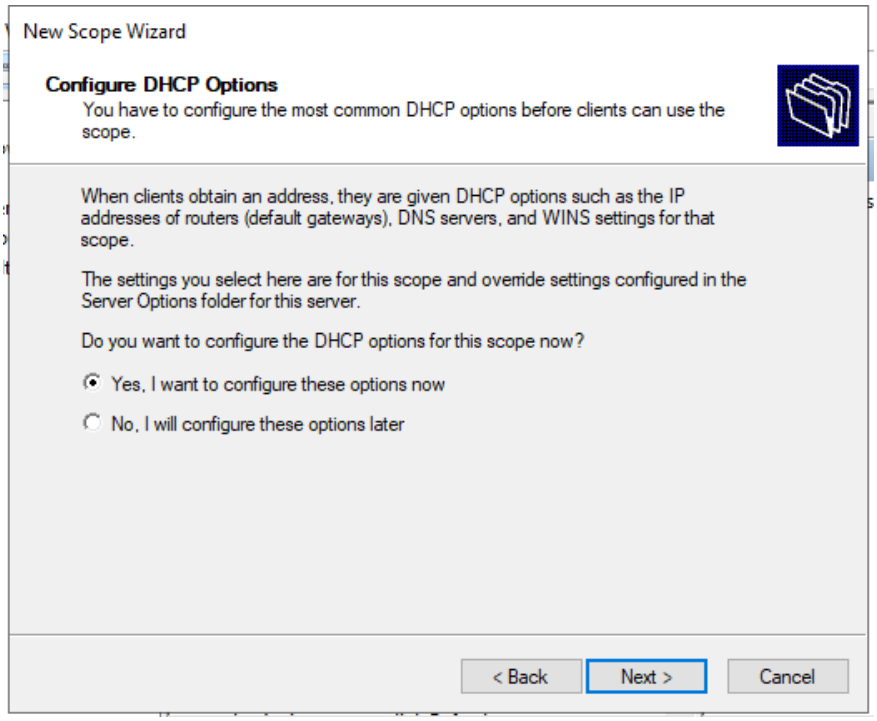
Obrázok 104 : Nastavenie rozsahu adries a masky (vlastný zdroj)

Ďalej pokračuje sprievodca možnosťou nastavenia adries, ktoré nemajú byť prideľované (teda sú vyhradené na iný účel, ako napríklad statické adresy). Keďže bol zvolený rozsah prideľovania od 100–200, tak do .100 sa adresy prideľovať nebudú, a je možné ich ľubovoľne využívať, takže tento parameter nie je potrebné nastavovať.



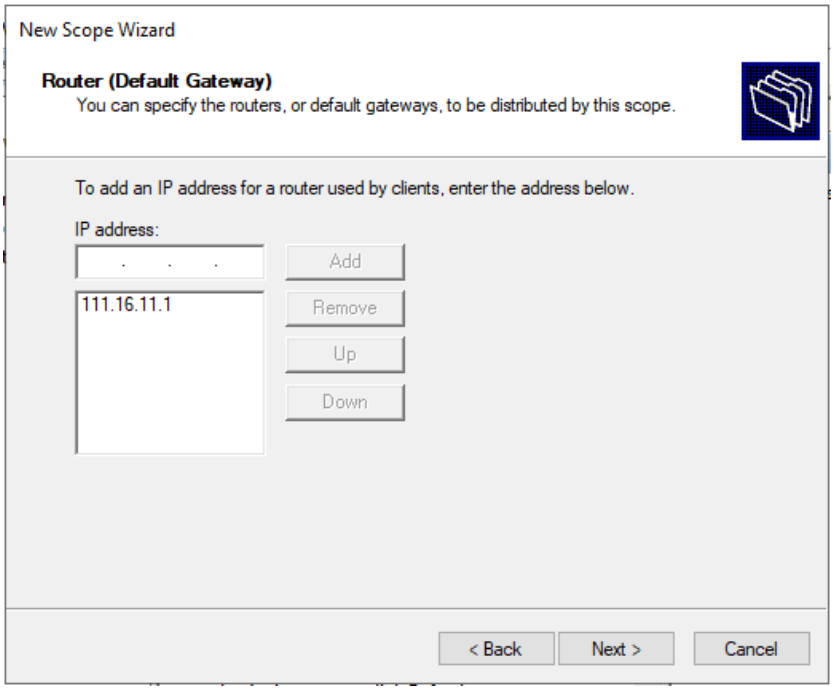
Obrázok 105 : Nastavenie vyhradených adries (vlastný zdroj)

Následne sprievodca inštaláciou dáva možnosť nastavenia role dokončiť, alebo len uložiť rozsah a nastavenia dokončiť neskôr. Zvolená bola možnosť dokončenia konfigurácie.



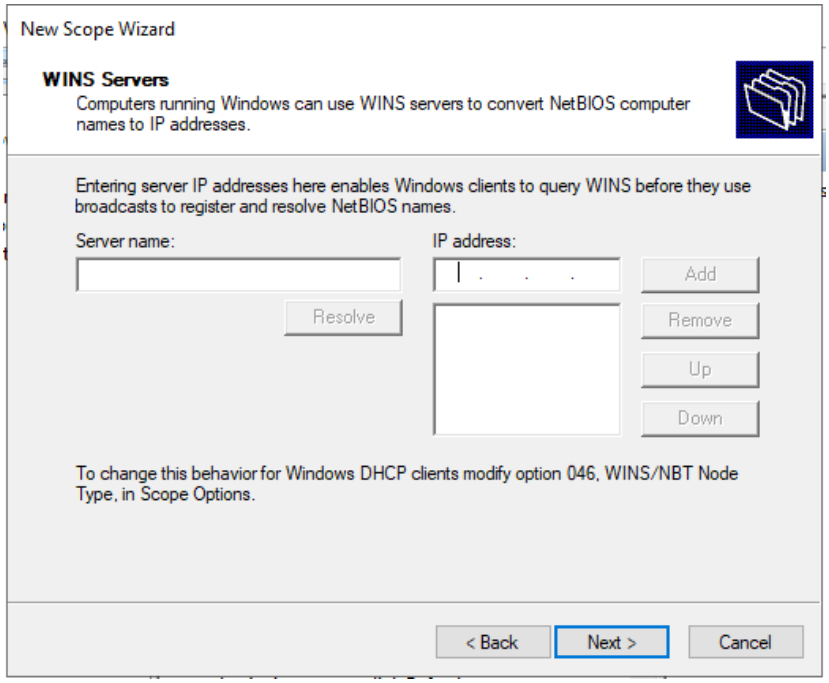
Obrázok 106 : Pokračovanie v konfigurácii nastavení (vlastný zdroj)

Ďalšou položkou pre nastavenie je nastaviť „Default Gateway“, čiže bránu. V tomto prípade je to testovací router, ktorý má IP adresu „111.16.11.1“.



Obrázok 107 : Nastavenie brány (vlastný zdroj)

Následne je možné zadať IP adresu WINS servera. Toto nastavenie sa práce netýka, v štruktúre konfigurovaný WINS server nie je, okrem toho je zastaraný a podporuje len platformu Windows.

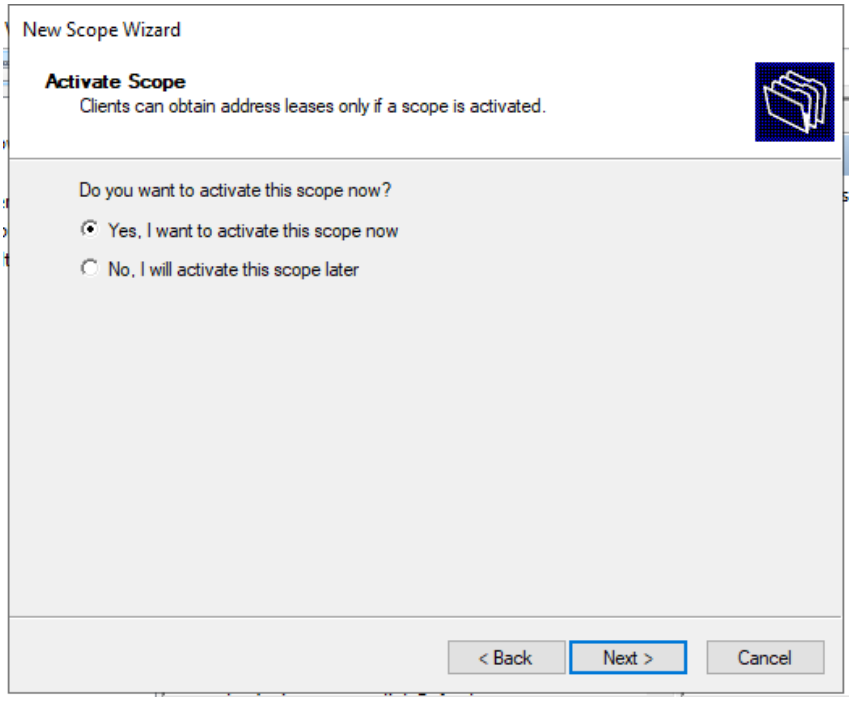


Obrázok 108 : Možnosť nastavenia IP adresy WINS (vlastný zdroj)

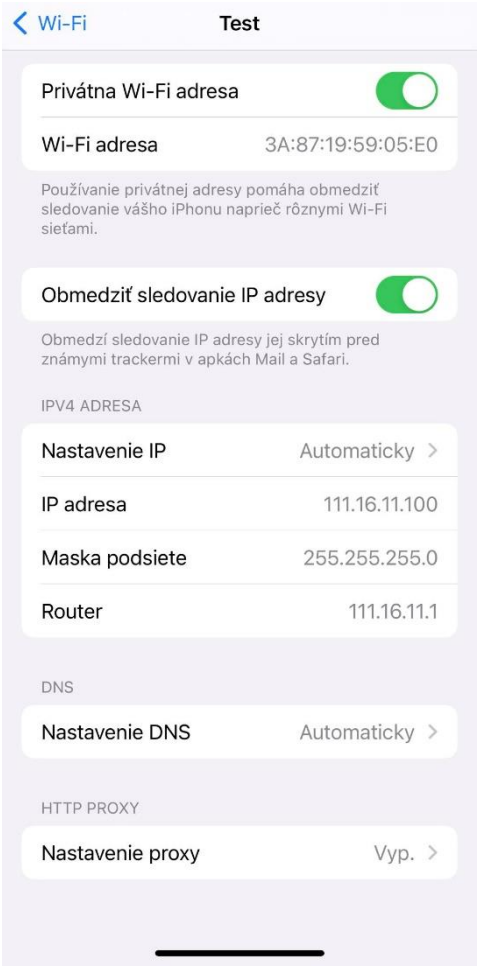
Poslednou položkou je možnosť nastavenia okamžitej aktivácie rozsahu, ktorá bude samozrejme zvolená. Nie vždy sa však rozsah aktivuje hneď, tu takisto platí, že po akejkoľvek konfigurácii je potrebné zariadenie reštartovať a otestovať správnosť konfigurácie.

Po tomto kroku je potrebné vypnúť DHCP prideľovanie na routri, aby sa jeho nastavenie nedostávalo do konfliktu s nastavením radiča.

Následne radič bude reštartovaný a otestuje sa funkčnosť role DHCP na mobilnom zariadení iPhone 12, ktoré sa pripojí bezdrôtovo k testovacej sieti „Test“ a následne sa prejde do nastavení Wi-Fi, kde sú k dispozícii informácie o sieti.



Obrázok 109 : Aktivácia rozsahu (vlastný zdroj)



Obrázok 110 : Test – úspešný (vlastný zdroj)

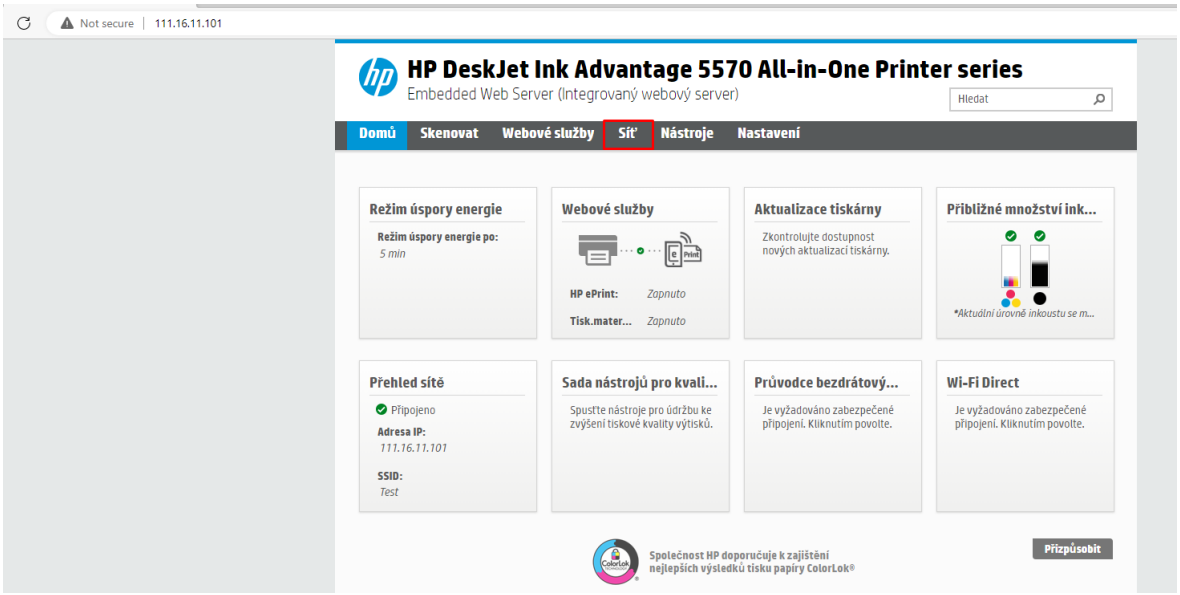
5.3.5 Konfigurácia role Print and Document Services

Vo firemnom prostredí je nutnosť využívania zdieľaných zdrojov, medzi ktoré patrí aj práve sieťová tlačiareň.

Ešte predtým, než sa začne rola „Print and Document Services“ konfigurovať, je potrebné zabezpečiť si ovládače pre danú tlačiareň – najlepšie priamo z oficiálnych stránok výrobcu.

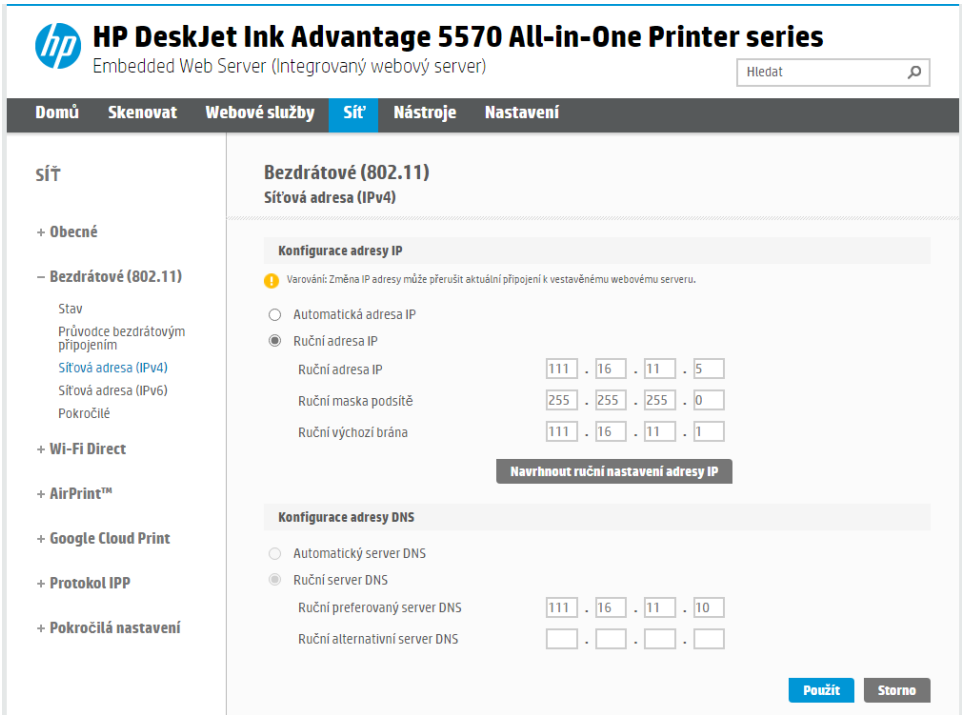
Tlačiareň použitá pre praktickú časť je od výrobcu HP, k ovládaču sa dá dostať veľmi jednoducho. Pre nahranie a deploy ovládača je však potrebné mať jeho správny formát, ktorým v tomto prípade nie je „.exe“ ale „.inf“ – teda je potrebné stiahnutý .exe súbor rozbaliť (napríklad pomocou programu 7zip). Ovládač bol stiahnutý z: https://support.hp.com/cz-cs/drivers/selfservice/hp-deskjet-ink-advantage-5570-all-in-one-printer-series/7234983/model/7234984. Konfigurácia teda v tejto chvíli môže započať. Začne sa nastavením statickej IP adresy tlačiarne, ku ktorej sa pristúpi pomocou webového

rozhrania (momentálne sa jej pomocou DHCP pridelila adresa 111.16.11.101, je však potrebné jej prideliť adresu staticky z rozsahu, ktorý je mimo DHCP). Bola vybraná adresa 111.16.11.5.



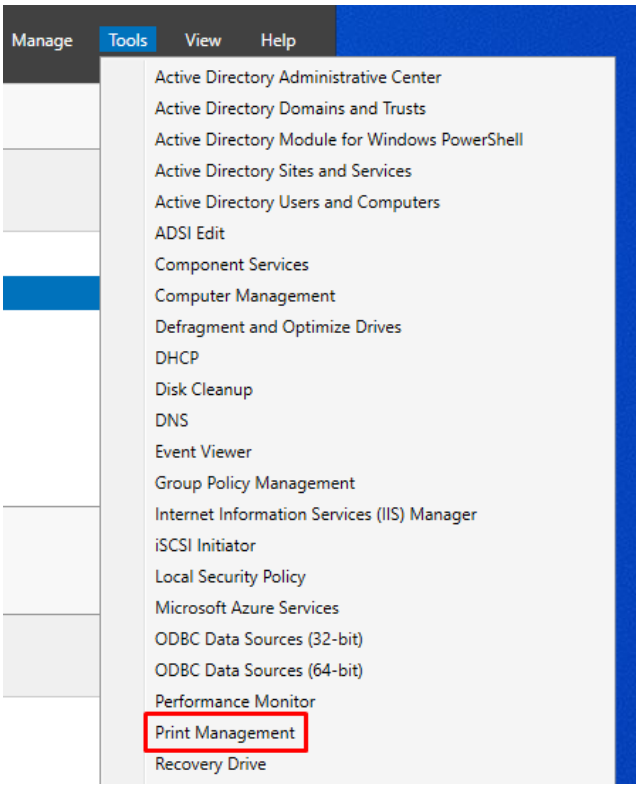
Obrázok 111 : Prístup k tlačiarni pomocou webového rozhrania (vlastný zdroj)

Pod záložkou „Síť“ v „Síťová adresa (IPv4“) je potrebné vybranú adresu staticky nastaviť.



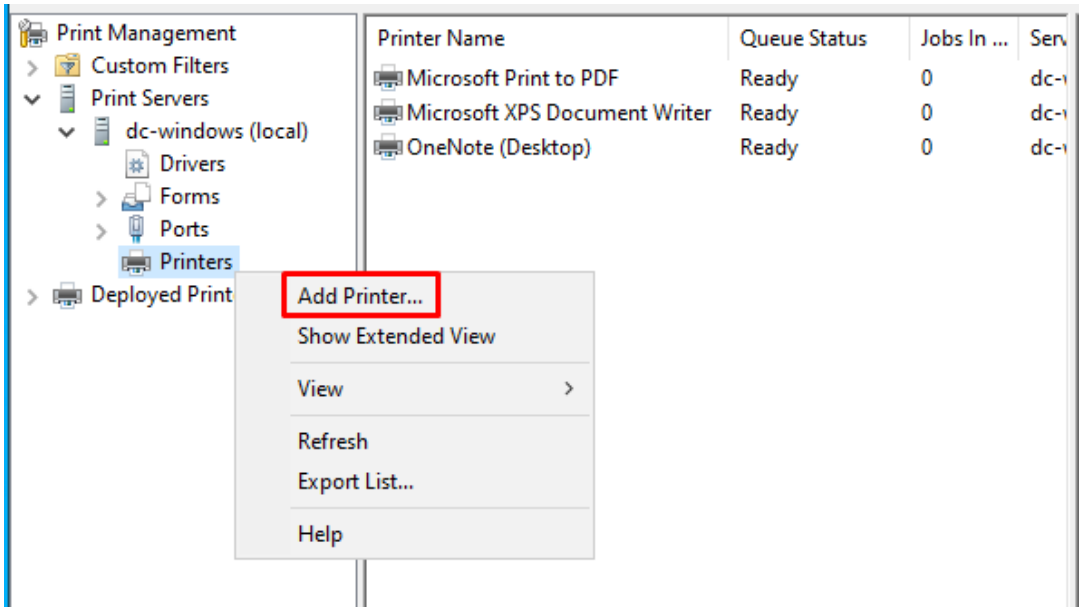
Obrázok 112 : Nastavenie statickej IP adresy na tlačiarni (vlastný zdroj)

Teraz je potrebné prejsť do „Server Manager“ a zo záložky „Tools“ vybrať možnosť konfigurácie tlačových služieb.



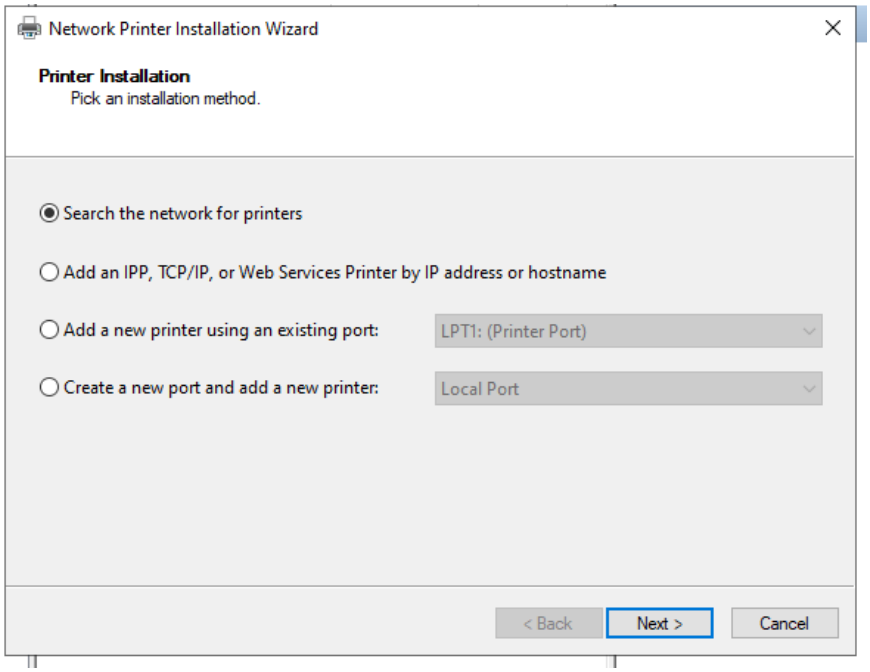
Obrázok 113 : Začiatok konfigurácie role Print and Documents Service (vlastný zdroj)

Teraz nasleduje krok pridania tlačiarne, štandardne kliknutím pravého tlačidla na „Printers“ a možnosť „Add Printer“



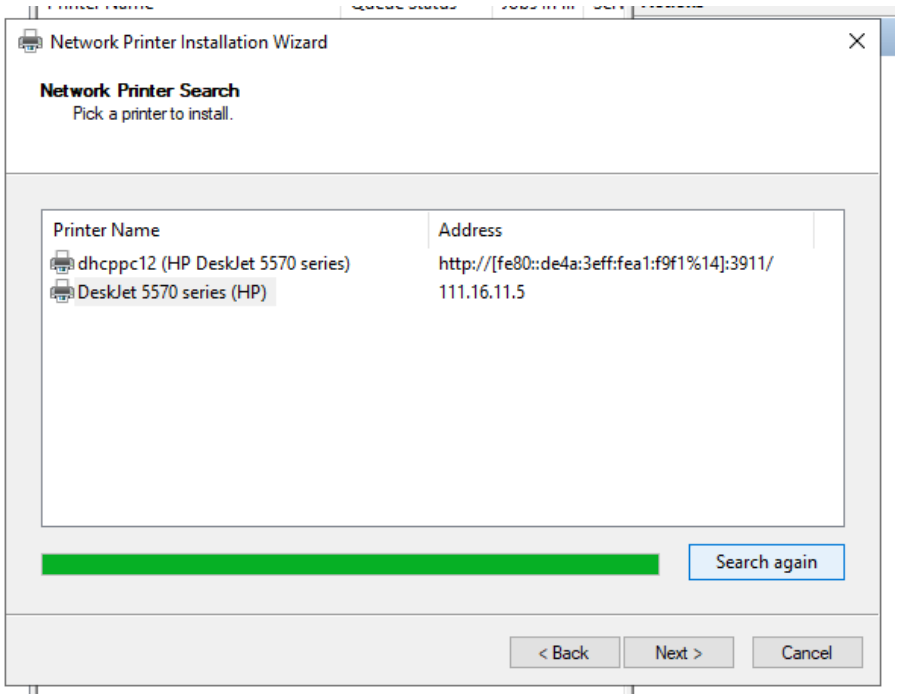
Obrázok 114 : Pridanie novej tlačiarne (vlastný zdroj)

Tlačiareň je možné buď pridať manuálne, alebo existuje možnosť vyhľadávania tlačiarní v sieti, ktorá bude využitá.

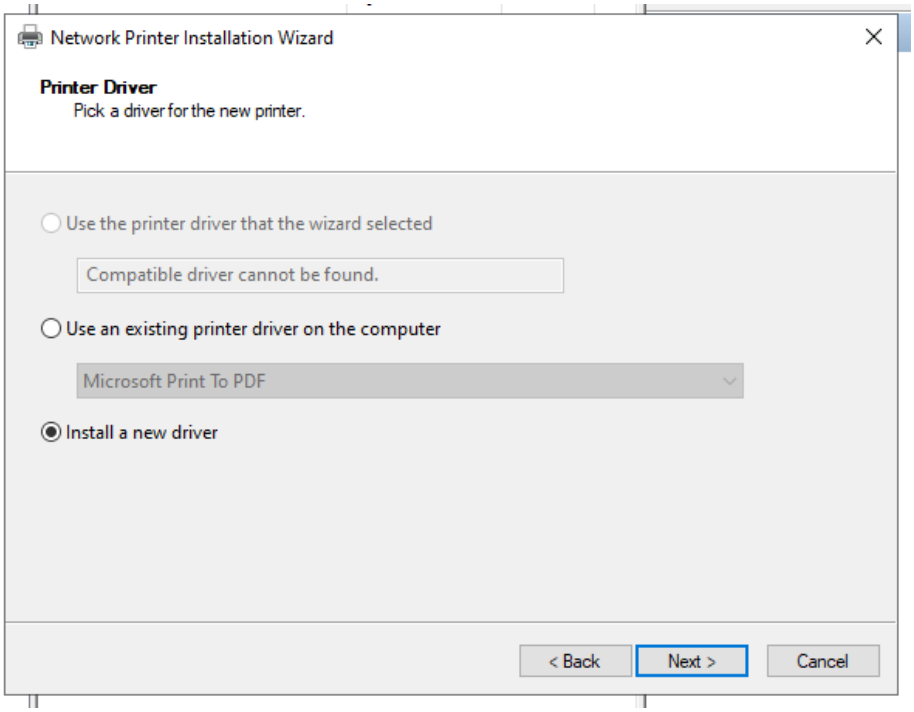


Obrázok 115 : Možnosti pridania tlačiarne (vlastný zdroj)

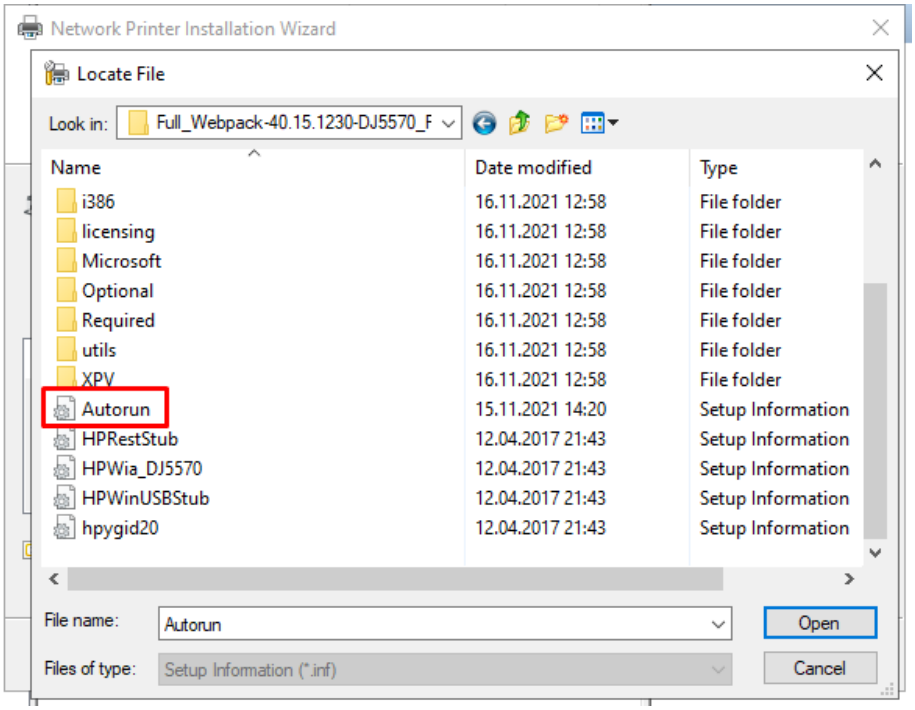
Sprievodca inštaláciou tlačiareň úspešne našiel, takže je možné sa presunúť k ďalšiemu kroku – výberu ovládača. Zvolí sa teda možnosť „Install a new driver“ a následne sa presunúť na lokalitu zložky s príslušným driverom.



Obrázok 116 : Úspešné nájdenie tlačiarne (vlastný zdroj)

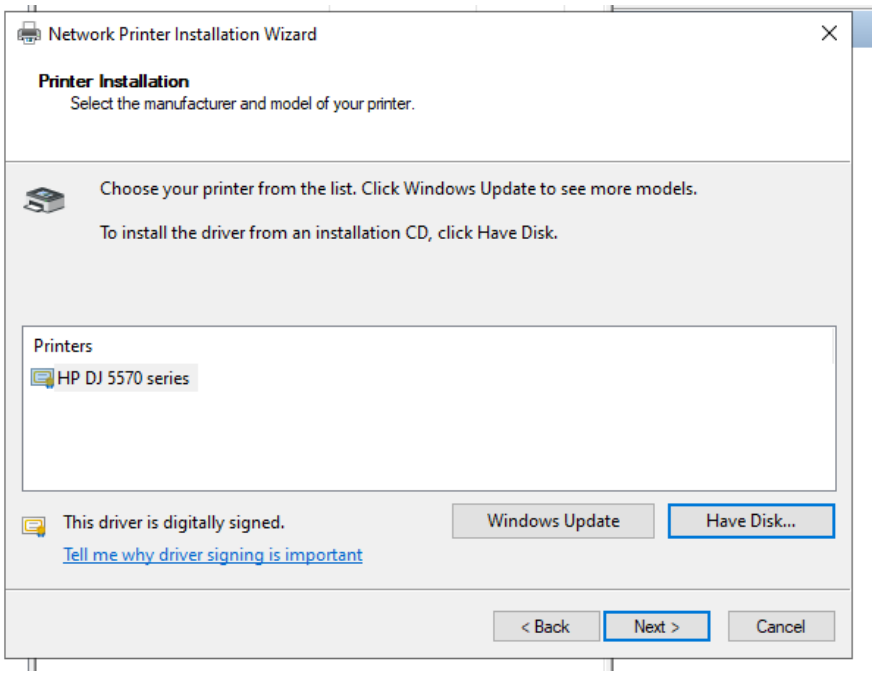


Obrázok 117 : Inštalácia nového ovládača (vlastný zdroj)



Obrázok 118 : Výber príslušného ovládača (vlastný zdroj)

Pokiaľ je ovládač kompatibilný s požiadavkami, sprievodca umožní ďalší krok.



Obrázok 119 : Ovládač spĺňa požiadavky (vlastný zdroj)

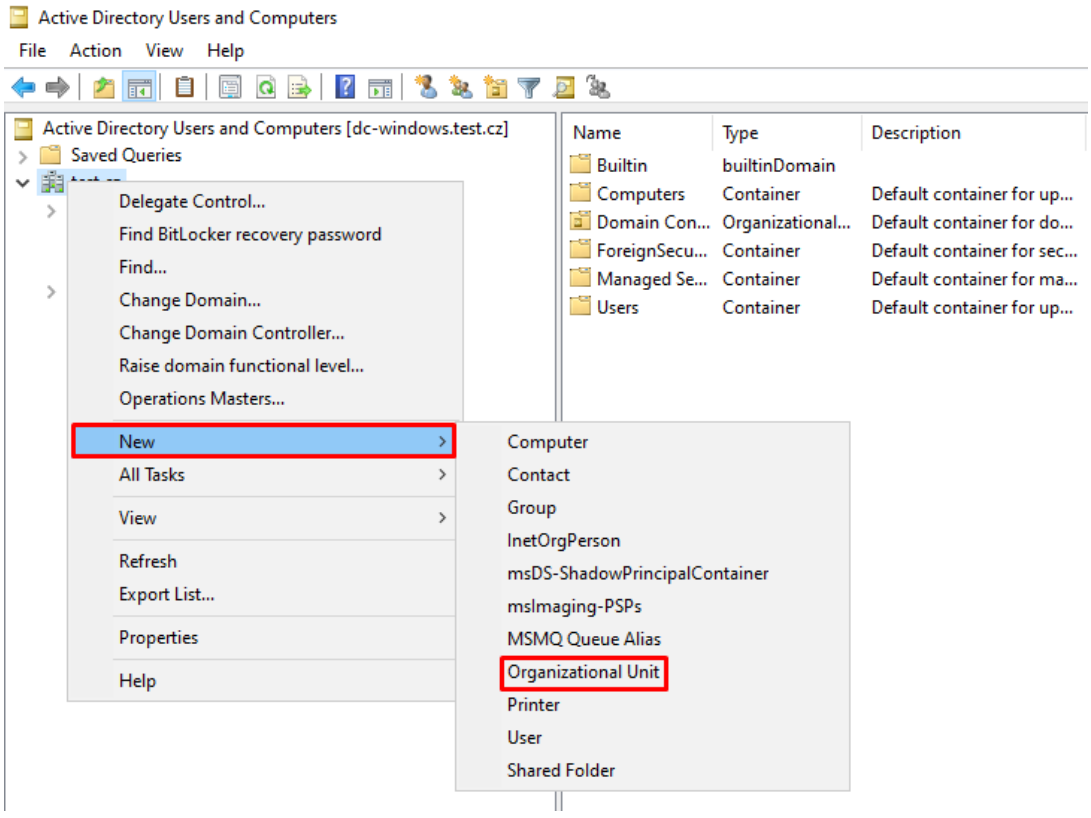
Po tomto kroku je možné vybrať si názov tlačiarne, pod ktorým bude dohľadateľná (napríklad „Tlačiareň pre oddelenie xyz“), avšak v tejto diplomovej práci figuruje len jedna tlačiareň, takže názov sa ponechá pôvodný.

Na konci inštalácie je možnosť vytlačenia testovacej stránky, ktorá prebehla v poriadku. Testovacia tlačiareň však nedisponuje tonerom, pretože sa testom funkčnosť bude práca zaoberať až pri finálnom testovaní nastavenia.

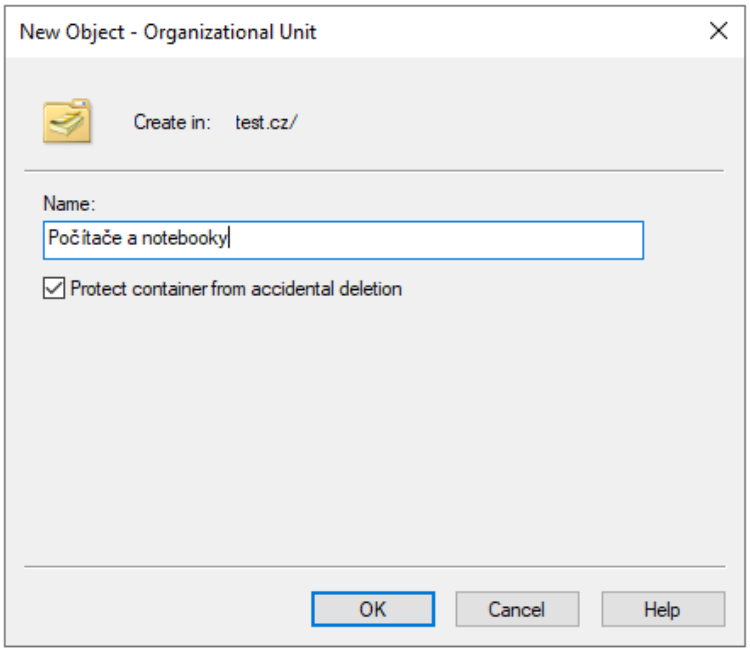
5.3.6 Konfigurácia role WSUS

Rola WSUS slúži pre automatické aktualizácie bez nutnosti zásahu administrátora. Podmienkou je však jej správna konfigurácia, ktorá sa v krátkom časovom úseku nedá otestovať (problémy môžu vyplávať na povrch kľudne aj pol roka po nastavení), preto je dôležité túto rolu zo začiatku nakonfigurovať tak, aby si administrátor mohol vyberať súčasti a balíčky na inštaláciu a aby sa inštalácia nerobila automaticky – pokiaľ sa časom zistí, že výber balíčkov bol správny, inštalácia aktualizácií sa môže plne zautomatizovať.

Začiatok konfigurácie tejto role je iný, než pre predošlé role – rola WSUS potrebuje pre svoje fungovanie vytvorenie skupinovej politiky. Avšak ešte pred vytvorením politiky je potrebné vytvoriť OU, do ktorej budú spadať všetky počítače a notebooky.

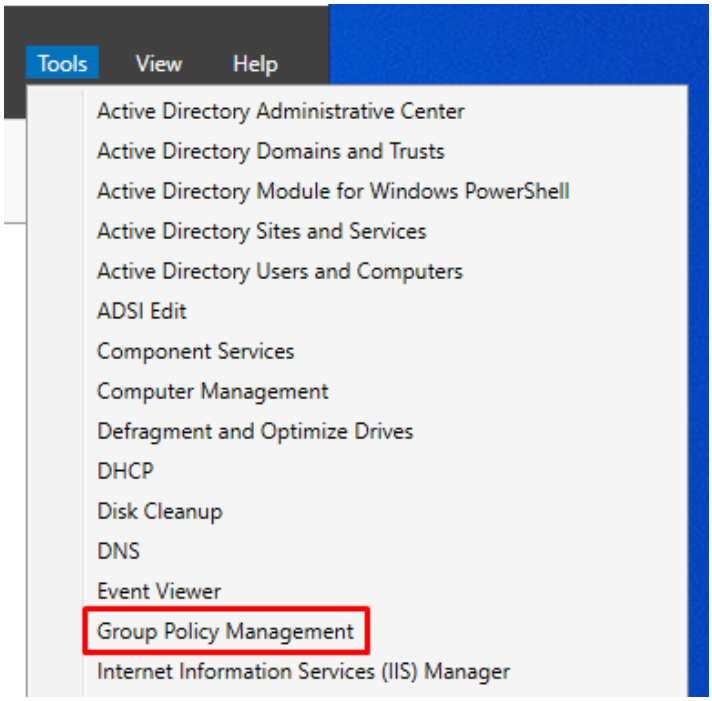


Obrázok 120 : Vytvorenie novej OU (vlastný zdroj)

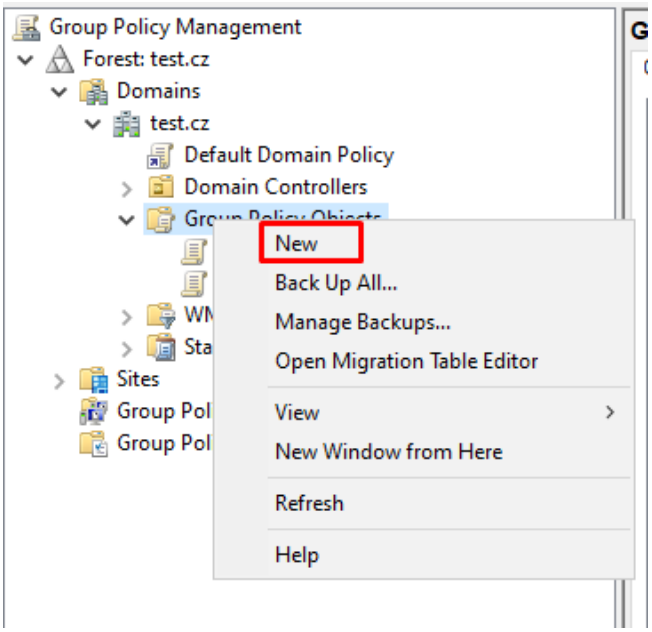


Obrázok 121 : Nastavenie názvu OU (vlastný zdroj)

Po vytvorení organizačnej jednotky je potrebné premiestniť všetky zariadenia zo zložky „Computers“ – tam sa nachádzajú všetky zariadenia, ktoré sa pripoja k doméne. Momentálne tam žiadne zariadenia nie sú. Po tomto kroku nasleduje konfigurácia skupinovej politiky pre WSUS.

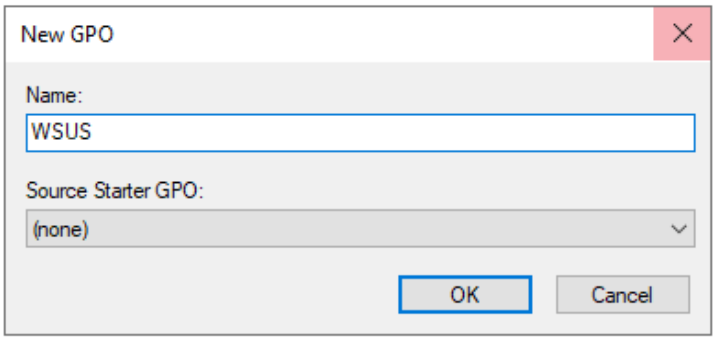


Obrázok 122 : Začiatok konfigurácie GPO pre WSUS (vlastný zdroj)



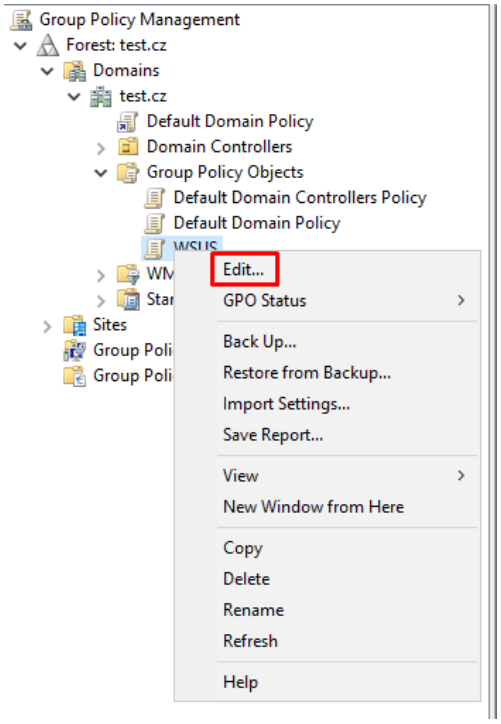
Obrázok 123 : Vytvorenie nového GPO (vlastný zdroj)

Ďalej je potrebné nastaviť názov GPO – tématicky „WSUS“.

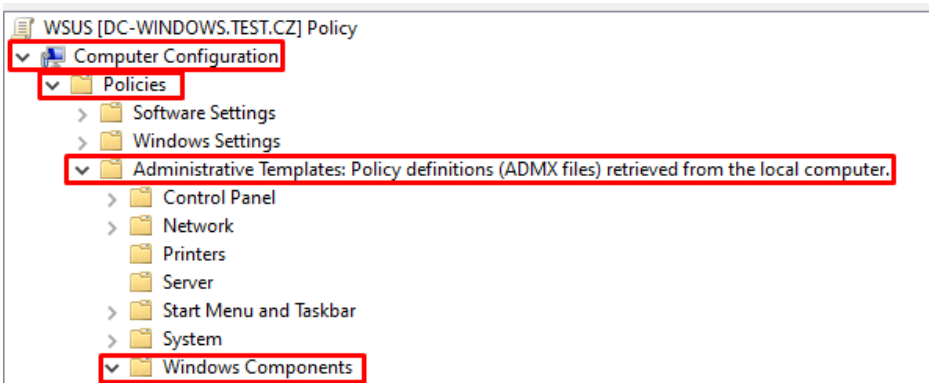


Obrázok 124 : Nastavenie názvu politiky (vlastný zdroj)

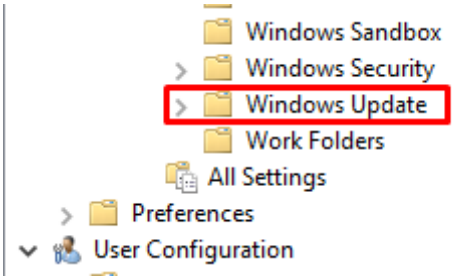
Následne je potrebné GPO konfigurovať. V tomto prípade je dôležitá konfigurácia pre zariadenie – WSUS aktualizuje konkrétne zariadenia užívateľov. Po kliknutí na možnosť „Edit“ užívateľ zistí, že je tam veľmi veľký počet položiek, pre ktoré sa dajú politiky konfigurovať, v tomto prípade je dôležitá položka „Windows Update“, do ktorej sa je potrebné preklikať.



Obrázok 125 : Začiatok editácie GPO (vlastný zdroj)



Obrázok 126 : Navigácia na položku „Windows Update“ 1 (vlastný zdroj)



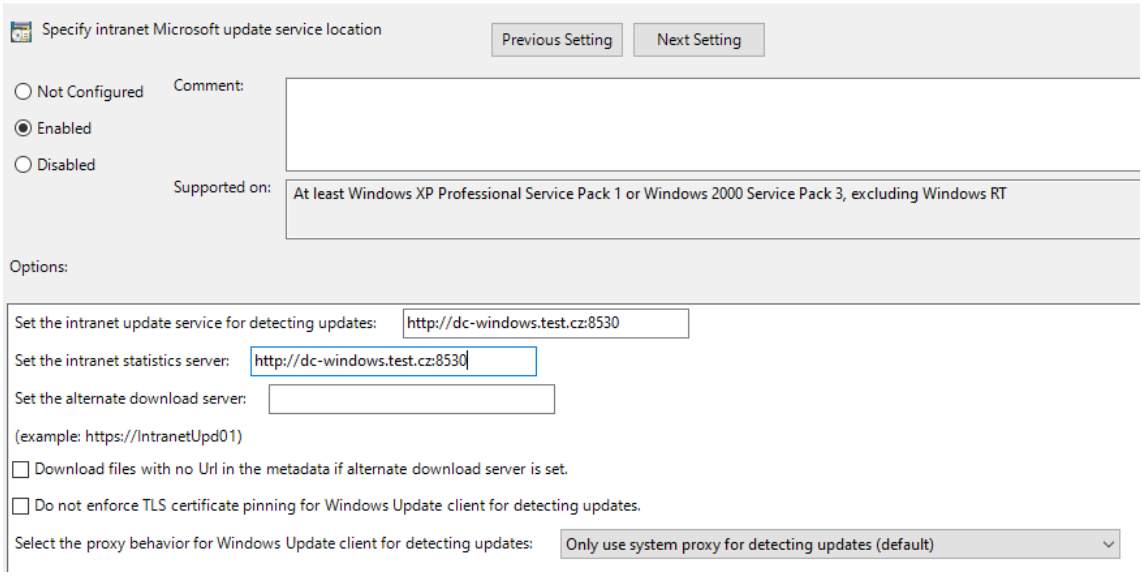
Obrázok 127 : Navigácia na položku „Windows Update“ 2 (vlastný zdroj)

Nasleduje vybrať politiky, ktoré bude potrebné konfigurovať, v tomto prípade sú to „Configure Automatic Updates“, „Specify intranet Microsoft update service location“ a „Automatic Updates detection frequency“.

Setting	State	Comment
Windows Update for Business		
Do not display 'Install Updates and Shut Down' option in Sh...	Not configured	No
Do not adjust default option to 'Install Updates and Shut Do...	Not configured	No
Enabling Windows Update Power Management to automati...	Not configured	No
Turn off auto-restart for updates during active hours	Not configured	No
Specify active hours range for auto-restarts	Not configured	No
Allow updates to be downloaded automatically over metere...	Not configured	No
Always automatically restart at the scheduled time	Not configured	No
Specify deadline before auto-restart for update installation	Not configured	No
Configure auto-restart reminder notifications for updates	Not configured	No
Turn off auto-restart notifications for update installations	Not configured	No
Configure auto-restart required notification for updates	Not configured	No
Configure Automatic Updates	Not configured	No
Specify deadlines for automatic updates and restarts	Not configured	No
Specify intranet Microsoft update service location	Not configured	No
Automatic Updates detection frequency	Not configured	No
Do not allow update deferral policies to cause scans against ...	Not configured	No
Remove access to "Pause updates" feature	Not configured	No
Remove access to use all Windows Update features	Not configured	No
Do not connect to any Windows Update Internet locations	Not configured	No
Allow non-administrators to receive update notifications	Not configured	No
Specify Engaged restart transition and notification schedule ...	Not configured	No
Do not include drivers with Windows Updates	Not configured	No
Turn on Software Notifications	Not configured	No
Allow Automatic Updates immediate installation	Not configured	No
Turn on recommended updates via Automatic Updates	Not configured	No
No auto-restart with logged on users for scheduled automat...	Not configured	No
Re-prompt for restart with scheduled installations	Not configured	No
Delay Restart for scheduled installations	Not configured	No
Reschedule Automatic Updates scheduled installations	Not configured	No
Configure auto-restart warning notifications schedule for u...	Not configured	No
Update Power Policy for Cart Restarts	Not configured	No
Enable client-side targeting	Not configured	No
Allow signed updates from an intranet Microsoft update ser...	Not configured	No
Display options for update notifications	Not configured	No

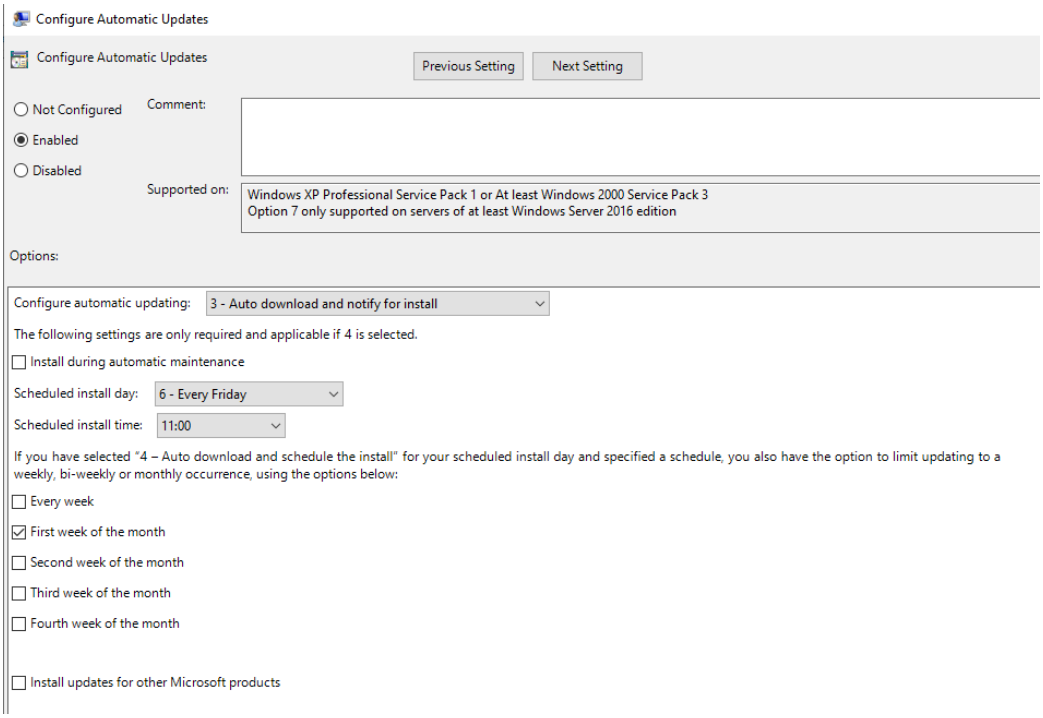
Obrázok 128 : Výber politík pre konfiguráciu (vlastný zdroj)

Je jedno, ktorou politikou sa začne – zvolená bola „Specify intranet Microsoft update service location“. Politiky sa musia povoliť tlačidlom „Enable“ a prípadne konfigurovať, keď je na to možnosť (niektoré sú tak špecifické, že nie je potrebné im nastavovať žiadne parametre). Táto konkrétna politika slúži k špecifikovaniu, na aký server sa aktualizácie budú ukladať (myslí sa tým server vnútri siete, kde bude dochádzať k aktualizáciám).



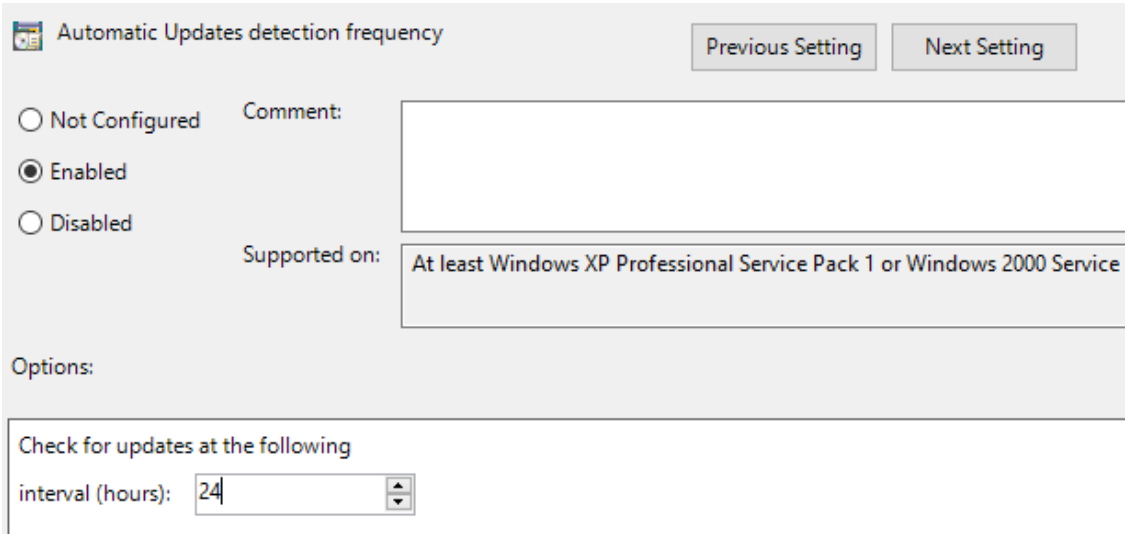
Obrázok 129 : Povolenie a nastavenie politiky „Specify intranet Microsoft update service location“ (vlastný zdroj)

Ako ďalšia politika sa konfiguruje „Automatic Updates“. V tejto politike sa nastavuje spôsob aktualizácie (teda či bude plne automatizovaná, manuálna, alebo kombinovaná) a ako často sa budú aktualizácie inštalovať. Toto nastavenie závisí na dohode vo firemnom prostredí. Neodporúča sa aktualizácie plne automatizovať, najprv je potrebné si odskúšať, či sa sťahujú vyhovujúce aktualizácie a či služba správne funguje.



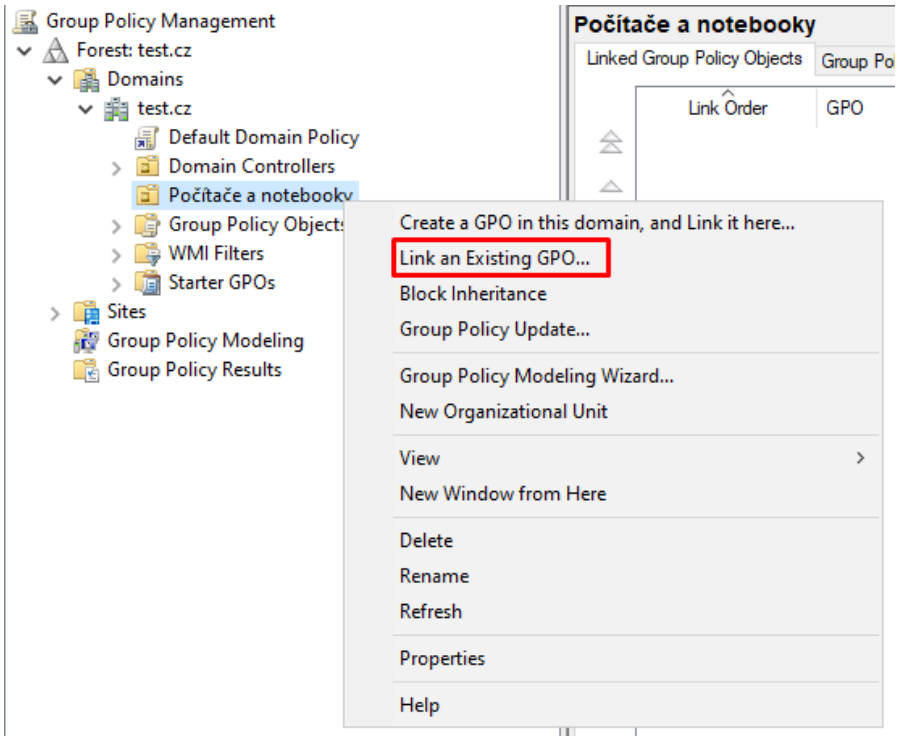
Obrázok 130 : Povolenie a nastavenie politiky „Windows Update“ (vlastný zdroj)

Ako posledná politika sa nakonfiguruje „Automatic Updates detection frequency“. Táto politika slúži k nastaveniu častosti vyhľadávania aktualizácií.

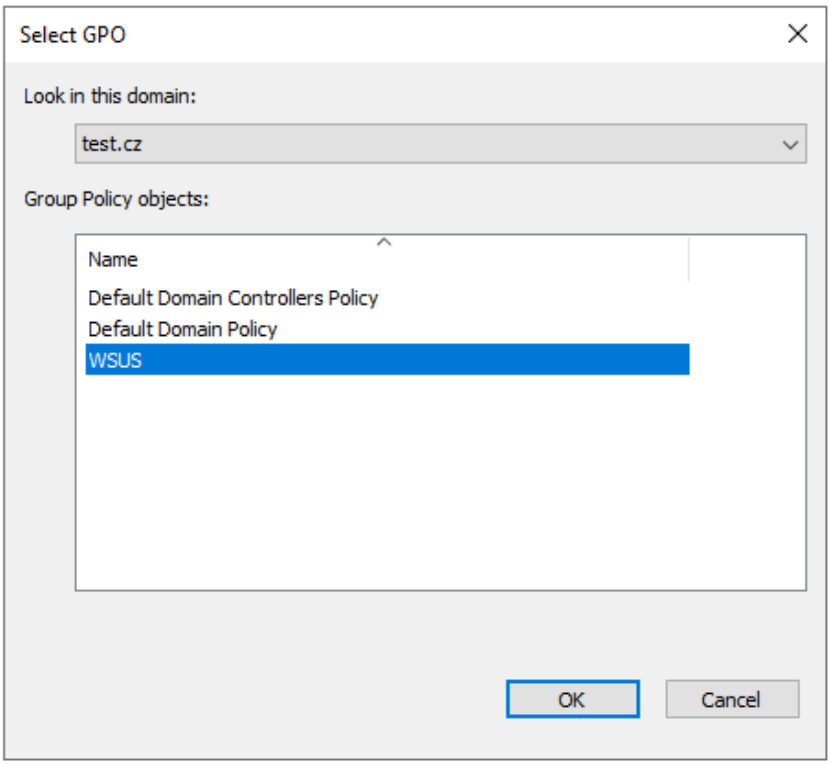


Obrázok 131 : Povolenie a nastavenie politiky „Windows Update detection frequency“ (vlastný zdroj)

V tejto chvíli sú politiky nastavené, teraz je potrebné vytvorené GPO „WSUS“ nalinkovať na organizačnú jednotku, pre ktorú bude daná politika platiť.

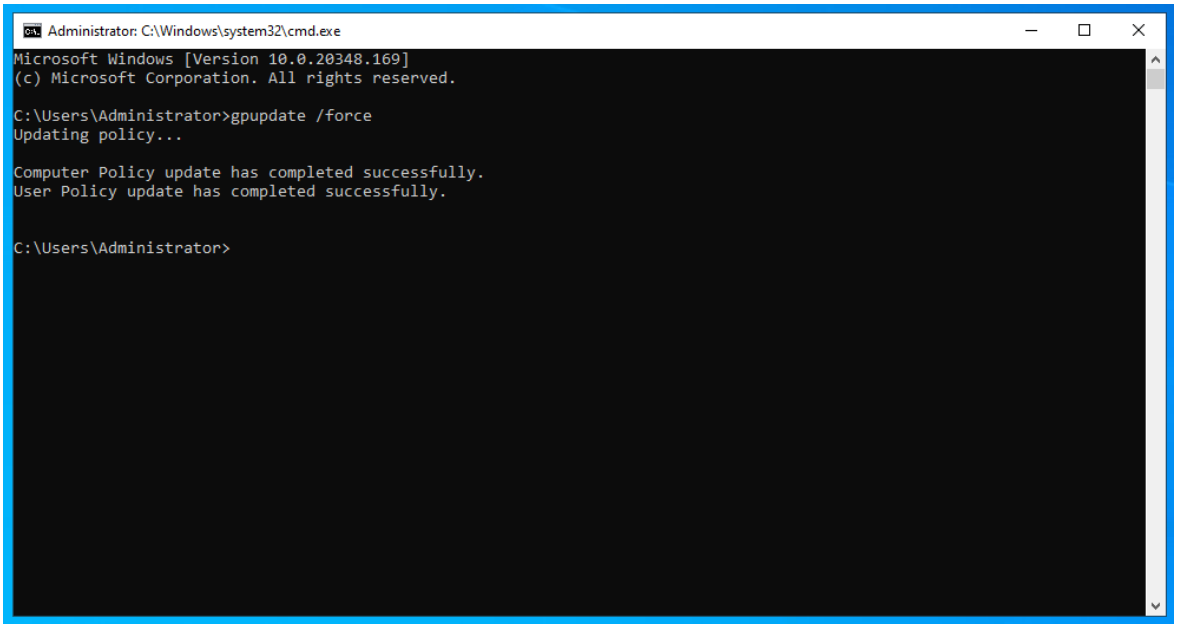


Obrázok 132 : Nalinkovanie politiky na príslušnú OU (vlastný zdroj)



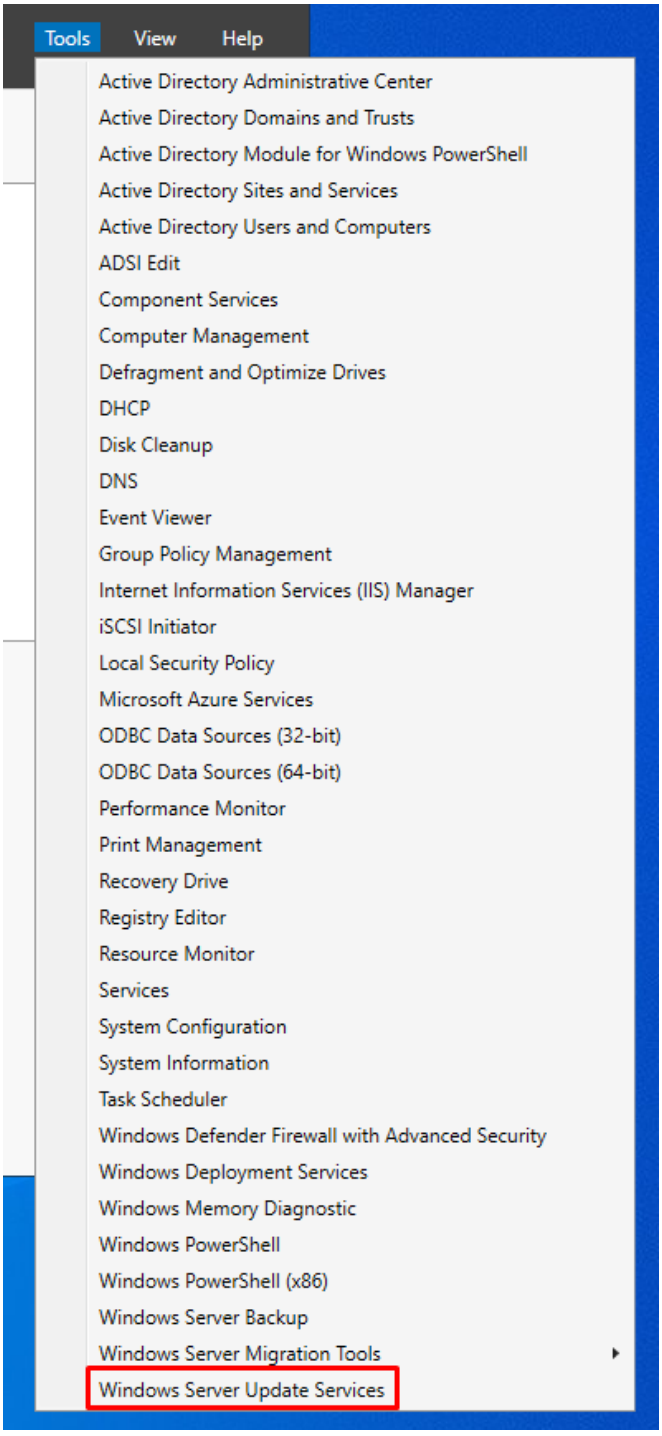
Obrázok 133 : Výber GPO pre linkovanie (vlastný zdroj)

Aby politika začala platiť, je potrebné buď reštartovať server (to je tá menej vhodná varianta), alebo reštartovať politiky pomocou príkazového riadku tak, ako na obrázku nižšie.

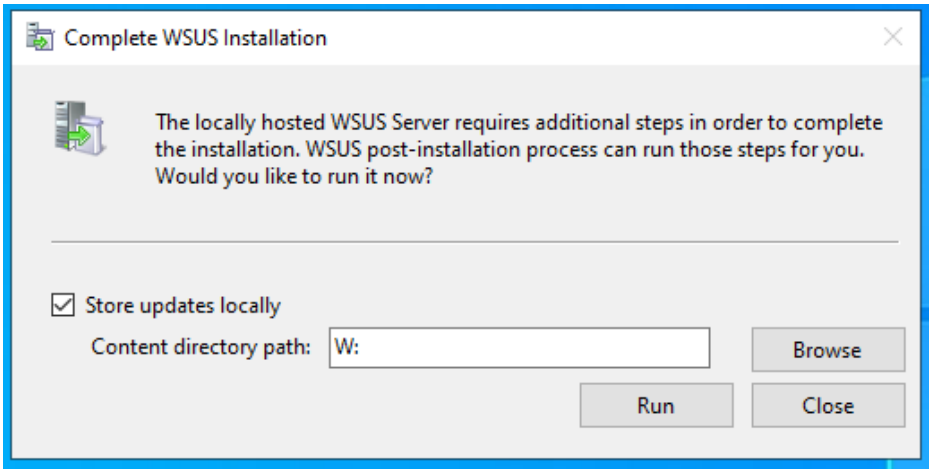


Obrázok 134 : Reštart politík (vlastný zdroj)

Teraz je potrebné už nainštalovanú rolu WSUS nakonfigurovať. Po stlačení tlačidla „Windows Server Update Services“ sa automaticky spustí sprievodca pre konfiguráciu role.

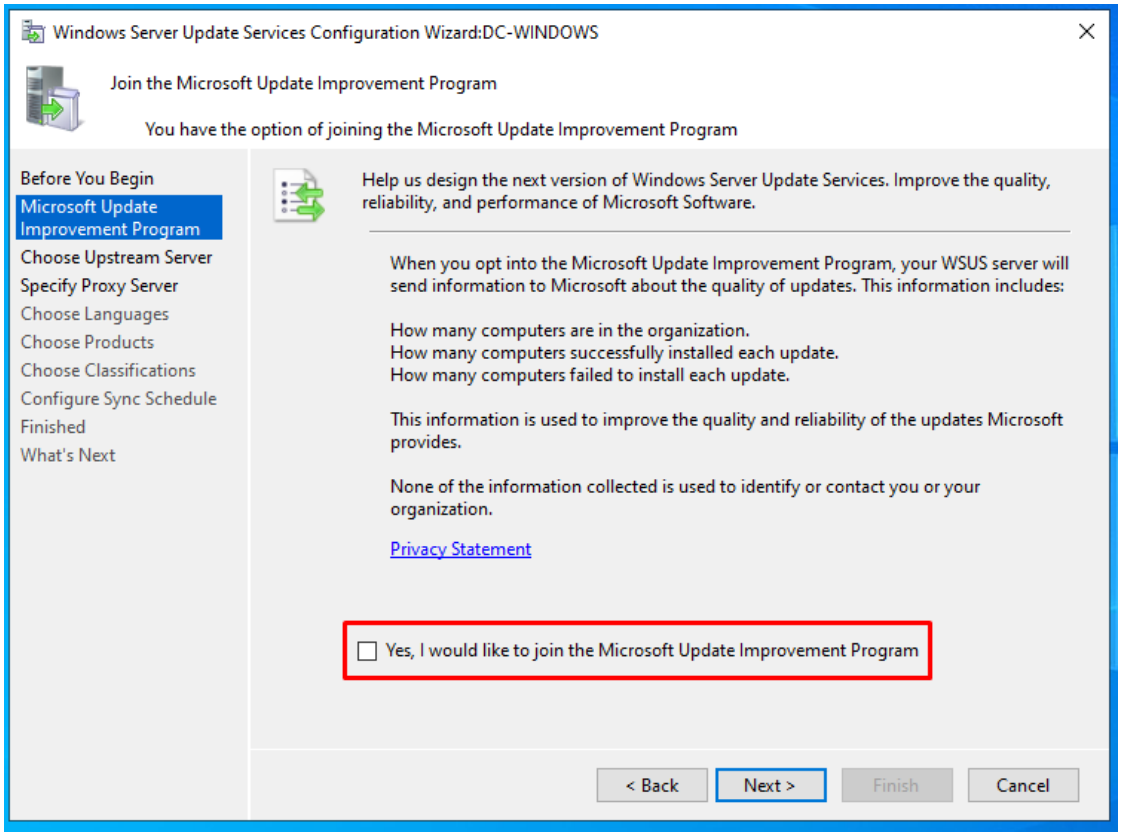


Obrázok 135 : Začiatok konfigurácie role WSUS (vlastný zdroj)



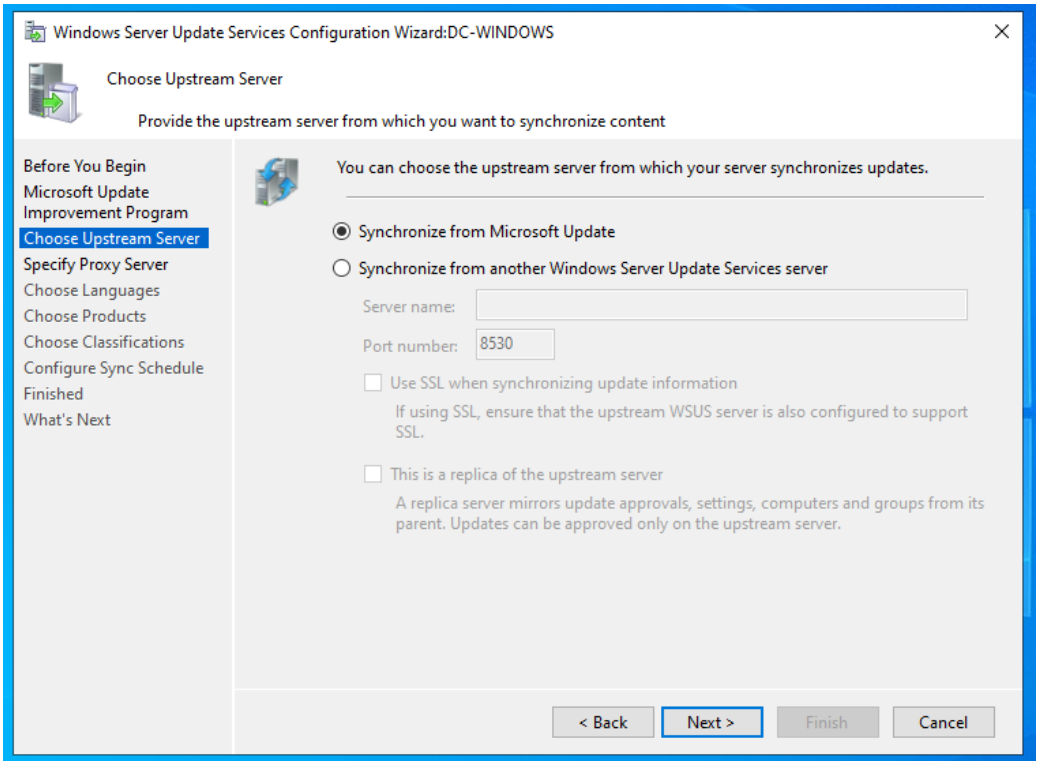
Obrázok 136 : Zvolenie umiestnenia pre ukladanie (vlastný zdroj)

Nasleduje dotaz pre pripojenie sa k programu „Microsoft Update Improvement Program“, táto možnosť povolená nebude.



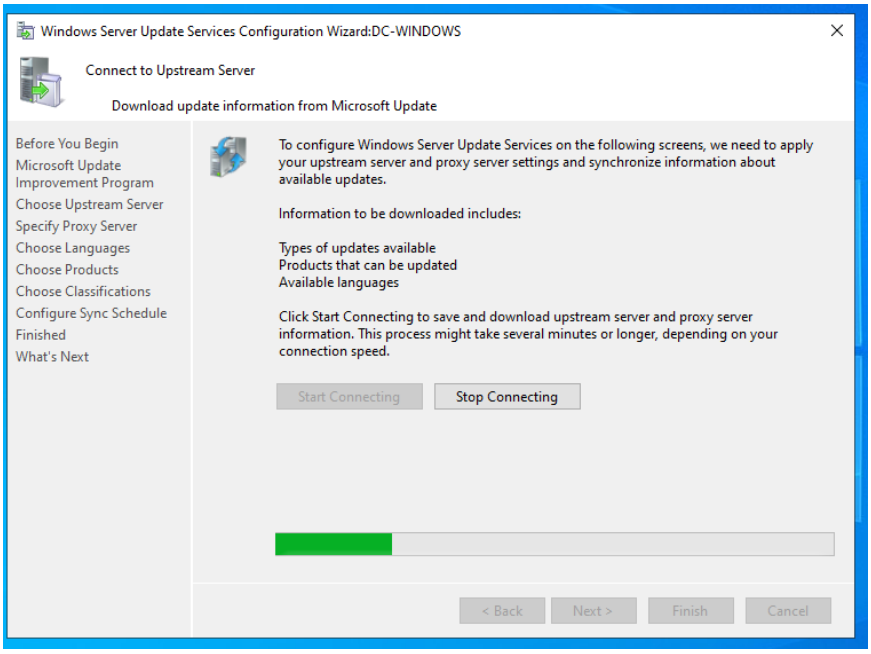
Obrázok 137 : Ponuka pre pripojenie sa k programu (vlastný zdroj)

Nasleduje možnosť výberu upstream serveru – to je server, z ktorého sa budú aktualizácie na radič sťahovať. Vybraná bola možnosť „Synchronize from Microsoft Update“.



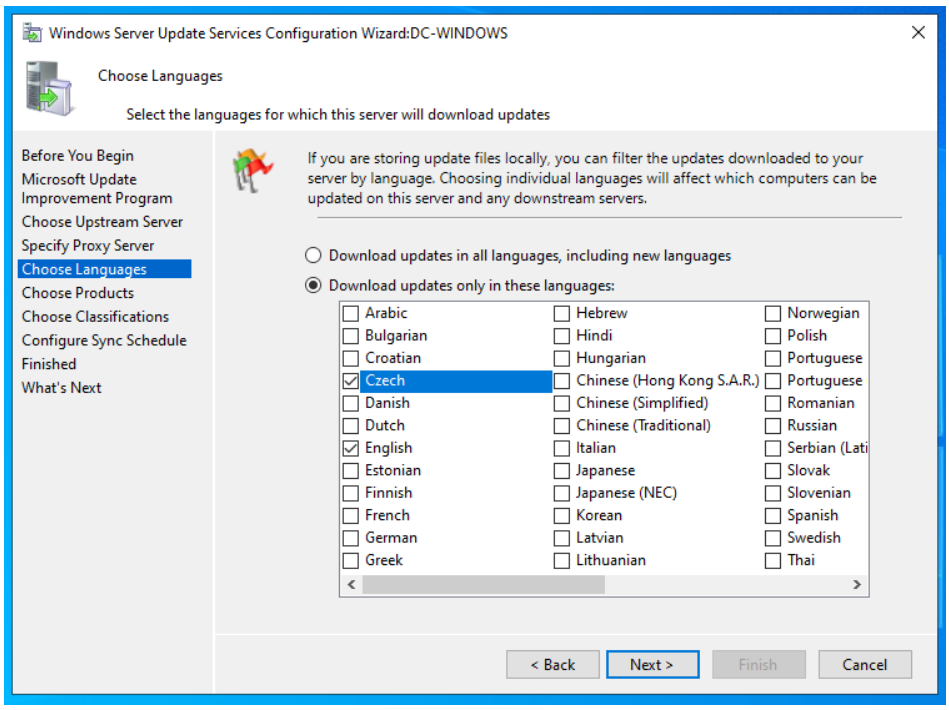
Obrázok 138 : Výber upstream serveru (vlastný zdroj)

Potom nasleduje medzikrok, ktorý sa práce netýka – a to je výber proxy servera pri prenose (týmto nastavením sa nie je potrebné zaoberať, pretože aktualizácie sa budú sťahovať priamo od Microsoftu). Po tejto špecifikácii sa server pokúsi spojiť so servermi Microsoftu.



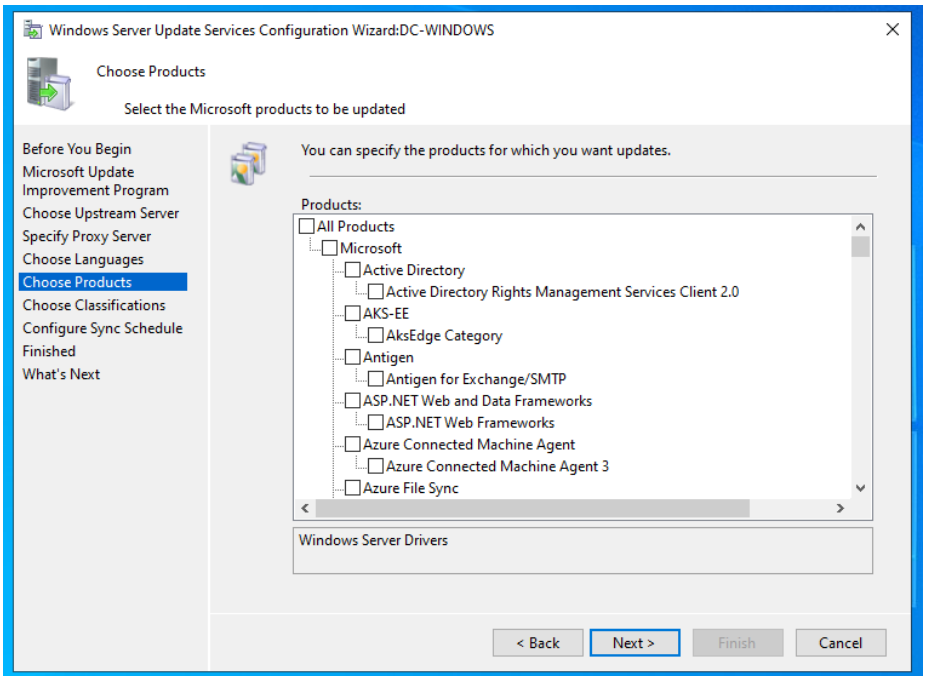
Obrázok 139 : Synchronizácia so servermi Microsoftu (vlastný zdroj)

Po tomto kroku nasleduje výber jazykov aktualizácií, ideálne je zvoliť jeden, maximálne dva a to z dôvodu kapacity na serveri, ale takisto z toho dôvodu, že užívateľovi sa stiahnu aktualizácie vo všetkých zvolených jazykov (pokiaľ sa teda nenastavia skupiny, ktoré by toto ošetrili).



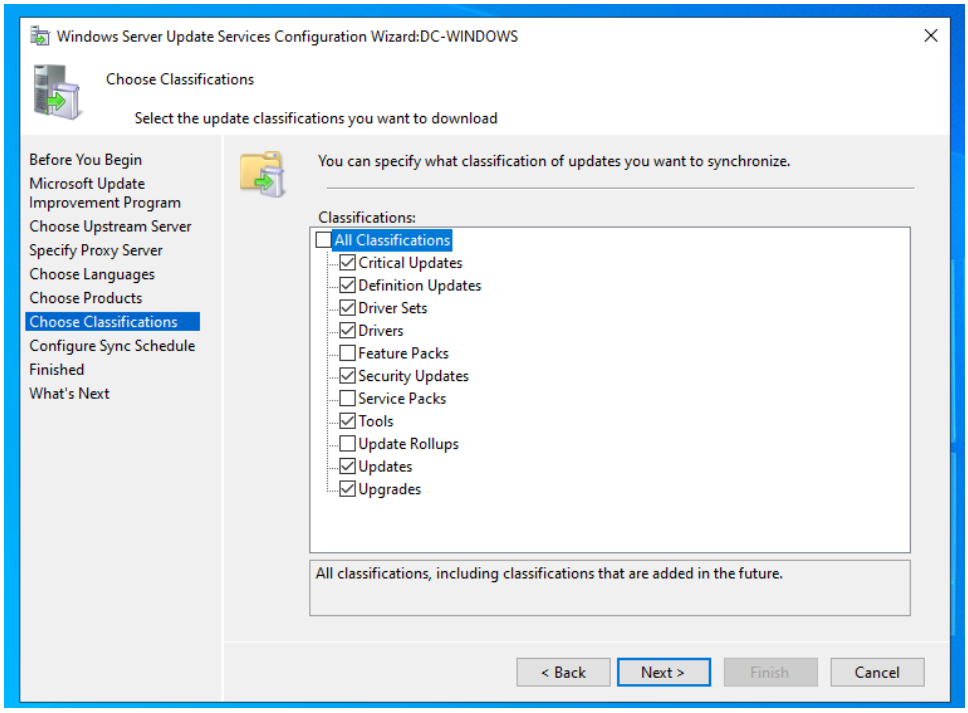
Obrázok 140 : Výber jazykov aktualizácií (vlastný zdroj)

Po tomto kroku je možné zvoliť si produkty na inštaláciu – pre prácu boli zvolené len produkty pre aktualizáciu Windows 10 a pre aktualizáciu súčastí serveru. Tých produktov je veľmi veľký počet a pre testovacie účely nemá zmysel vyberať všetky



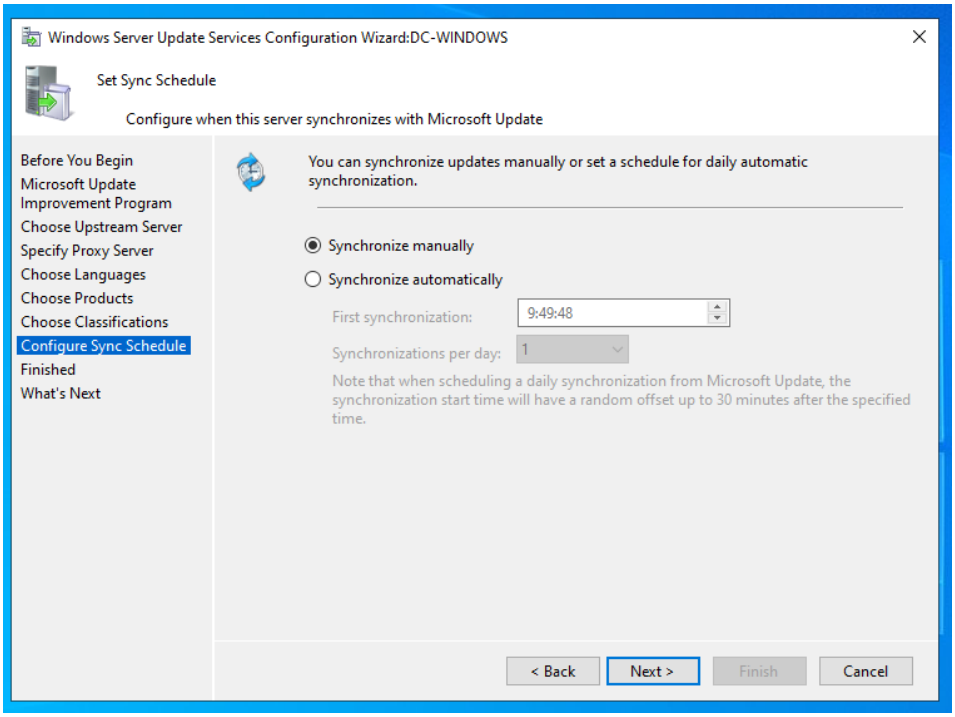
Obrázok 141 : Výber produktov (vlastný zdroj)

Vybrať sa dajú samozrejme aj klasifikácie.



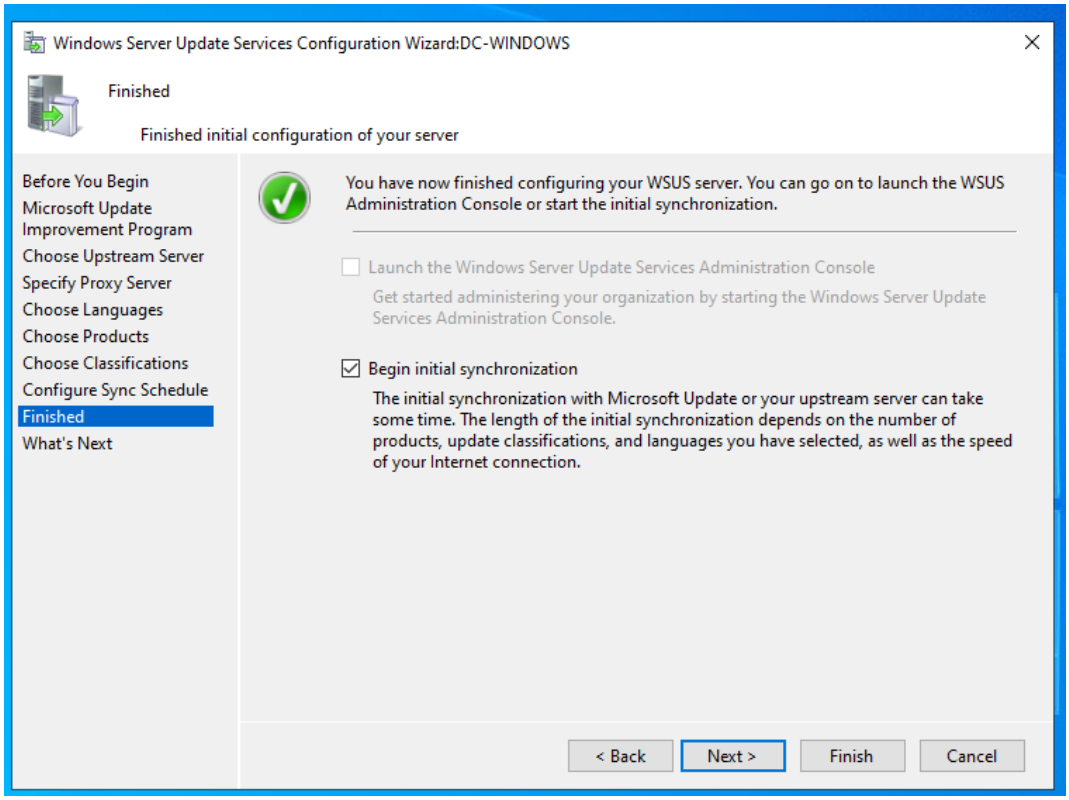
Obrázok 142 : Výber klasifikácií (vlastný zdroj)

Predposledným krokom je nastavenie synchronizácie – či sa bude synchronizovať manuálne alebo automaticky (s nastavením času). Táto synchronizácia sa týka spojenia s Microsoft servermi, odkiaľ budú sťahované aktualizácie.



Obrázok 143 : Nastavenie synchronizácie (vlastný zdroj)

Po tomto kroku nastane možnosť inicializačnej synchronizácie – teda priame spojenie s Microsoft servermi, odkiaľ sa začnú do vybraného úložiska sťahovať vybrané aktualizácie a súčasti z predošlých krokov. Tento krok zároveň trvá najdlhšie. Ako bolo spomenuté už na začiatku konfigurácie role WSUS, táto rola sa nedá okamžite otestovať, je to dlhodobá záležitosť.

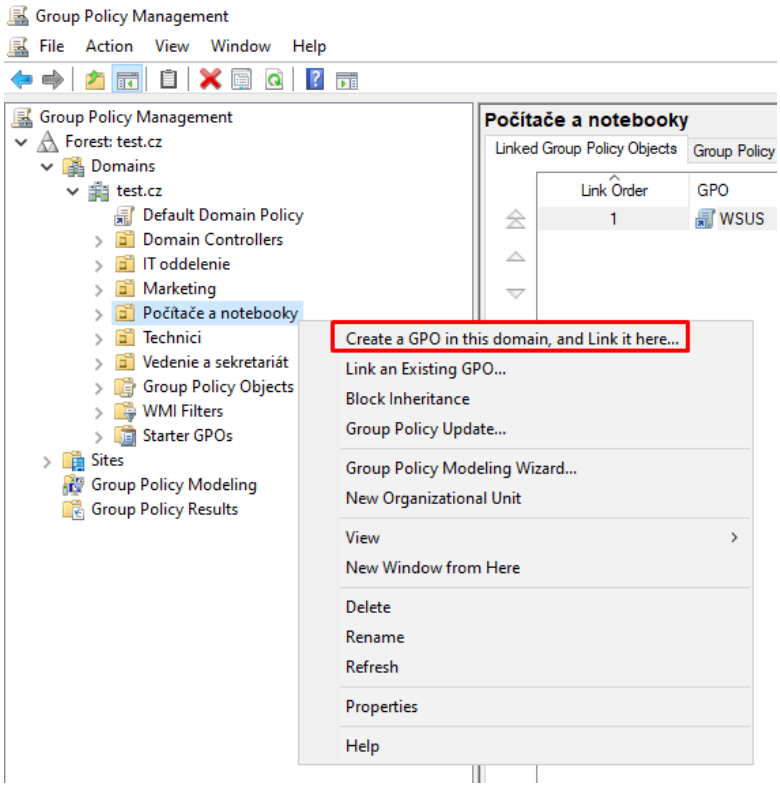


Obrázok 144 : Spustenie inicializačnej synchronizácie (vlastný zdroj)

5.3.7 Konfigurácia funkcie BitLocker

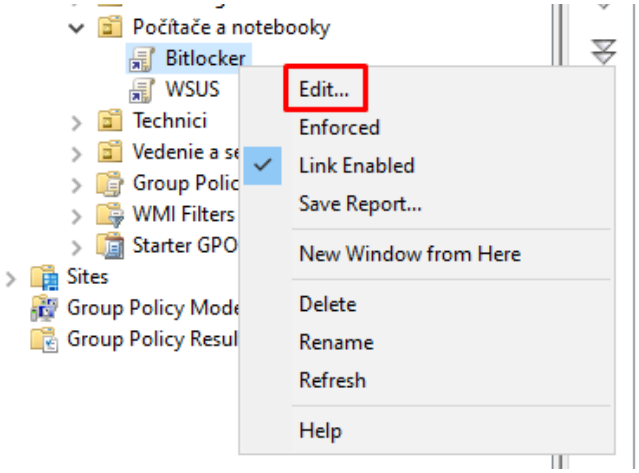
Ako bolo spomenuté už v minulých kapitolách, funkcie sa sami o sebe nemusia nastavovať, výnimkou je však funkcia BitLocker, ktorá potrebuje k svojmu fungovaniu nastaviť skupinovú politiku.

Táto GPO sa viaže ku konkrétnym zariadeniam, teda sa bude linkovať k OU „Počítače a notebooky“. U politiky je potrebné hneď na začiatok definovať jej názov, čo dokumentované nebude, názov bude „Bitlocker“

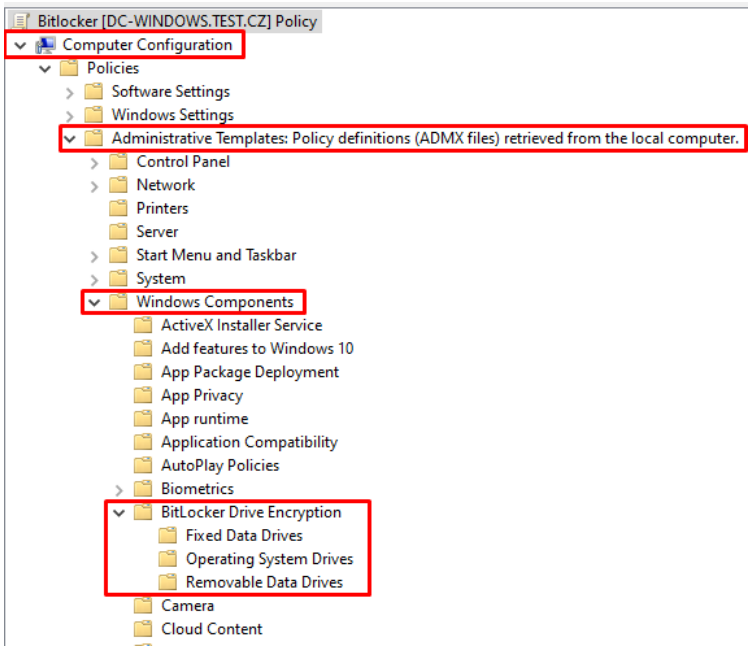


Obrázok 145 : Začiatok vytvorenia skupinovej politiky (vlastný zdroj)

Následne sa začne GPO editovať a politiky týkajúce sa BitLockeru sa nájdu v zložke „BitLocker Drive Encryption“.



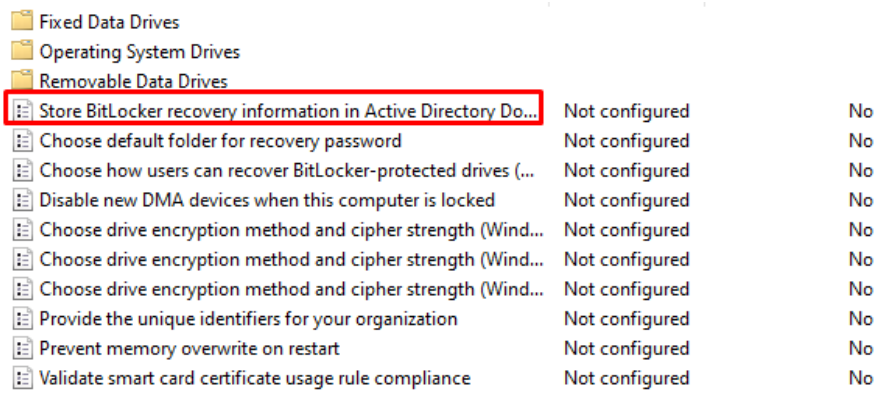
Obrázok 146 : Editovanie GPO (vlastný zdroj)



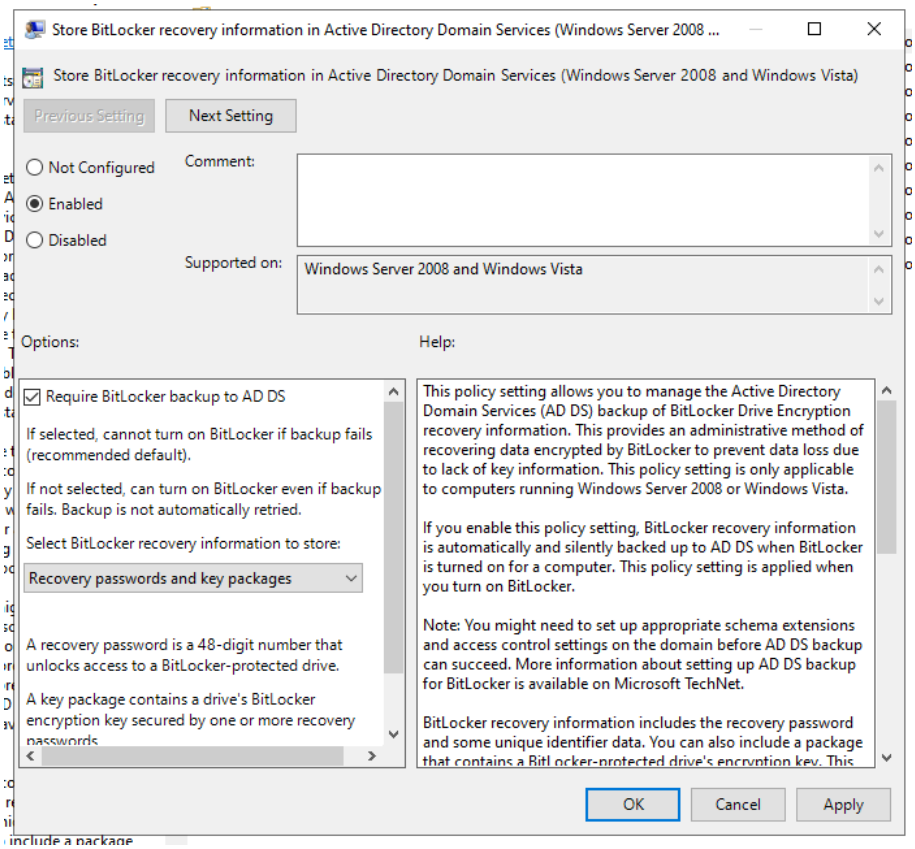
Obrázok 147 : Prejdenie na zložku „BitLocker“ Drive Encryption (vlastný zdroj)

Pre BitLocker je potrebné nakonfigurovať politiky: „Store BitLocker recovery information in Active Directory Domain Services“, „Allow network unlock on startup“ a „Choose how BitLocker – protected operating system drives can be recovered“.

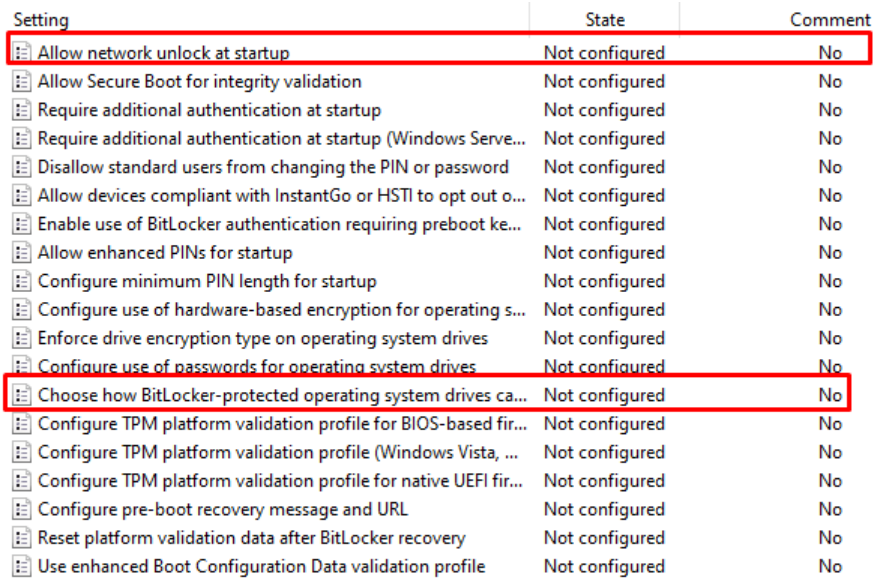
Táto politika definuje, či má dochádzať k ukladaniu kľúčov na doménovom radiči – to je dosť podstatné nastavenie, kľúče sa síce dajú uložiť na USB kľúč, ale toto nastavenie slúži ako ich záloha.



Obrázok 148 : Výber politiky „Store BitLocker recovery information in Active Directory Domain Services“ (vlastný zdroj)



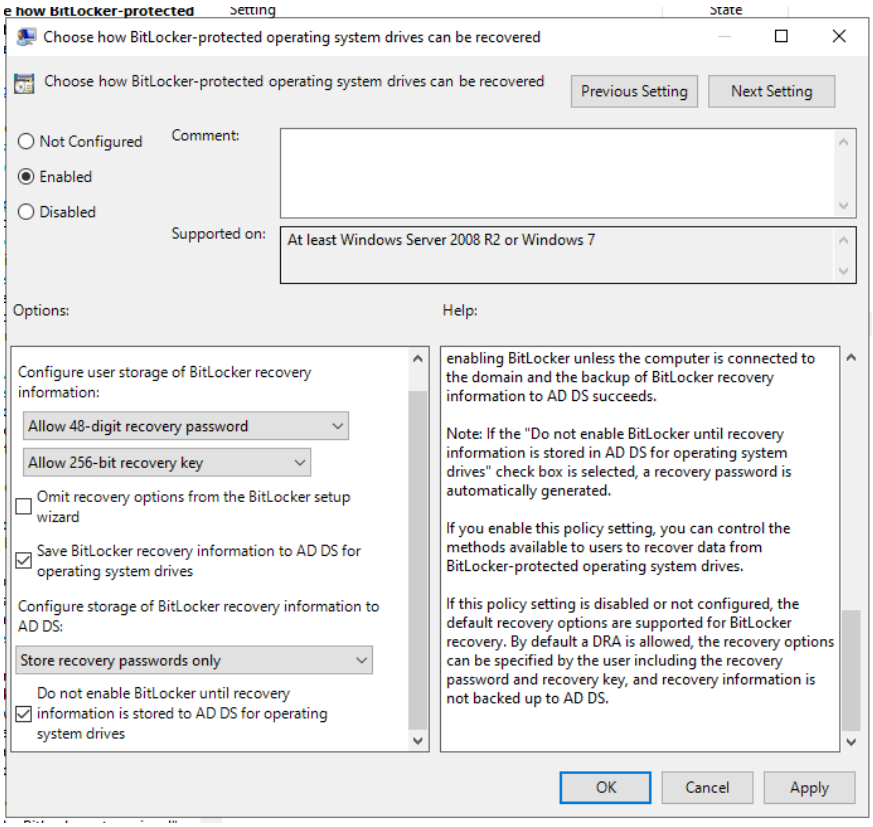
Obrázok 149 : Konfigurácia politiky „Store BitLocker recovery information in Active Directory Domain Services“(vlastný zdroj)



Obrázok 150 : Výber politík „Allow network unlock at startup“ a „Choose how BitLocker – protected operating system drives can be recovered“(vlastný zdroj

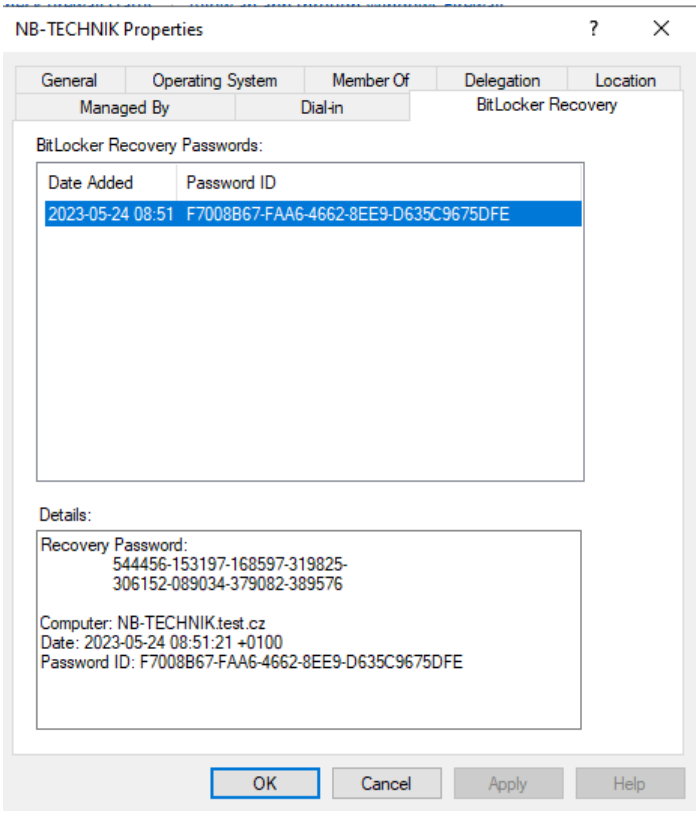
Politiku „Allow network unlock at startup“ je potrebné len zapnúť, nie je potrebná žiadna jej ďalšia konfigurácia, preto nebude dokumentovaná.

Avšak politika „Choose how BitLocker – protected operating system drives can be recovered“ potrebuje konfiguráciu.



Obrázok 151 : Konfigurácia politiky „Choose how BitLocker – protected operating system drives can be recovered“(vlastný zdroj)

BitLocker bol nastavený správne, po zašifrovaní testovacieho zariadenia sa na radiči v záložke „BitLocker Recovery“ nachádza kľúč.



Obrázok 152 : Recovery password zariadenia „NB-TECHNIK“(vlastný zdroj)

V praktickej časti boli vybrané aj funkcie „Windows Server Migration Tools “ a „Windows Server Backup“. Tieto funkcie však dokumentované nebudú a má to svoje dôvody. Tým prvým je, že je to kontraproduktívne – funkcie „Windows Server Migration Tools“ slúži na migráciu systému, čo táto diplomová práca nerieši a funkcia „Windows Server Backup“ sa nedá realizovať, keďže nie je k dispozícii ďalšie zariadenie, kam by sa server mohol zálohovať. Uvedené sú však v praktickej časti preto, pretože sú veľmi dôležité.

Najmä zálohovanie je dôležité – na to sa práve hodí backup server, ktorý sa spustí v prípade, že zlyhá pôvodný doménový radič. Backup servery sú dôležité pre reálnu prevádzku, táto diplomová práca sa však zaoberá testovacím radičom, ktorý v reálnej prevádzke však nikdy nebude.

5.4 Zabezpečenie doménového radiča a jeho zdrojov

Spôsoby, akými je možné doménový radič zabezpečiť je veľmi veľa – to by musela byť samostatná diplomová práca. Doménový radič je jednak potrebné zabezpečiť zvonku (teda správnou konfiguráciou routra a firewallu) a takisto zvnútra.

V tejto časti budú rozoberané spôsoby ochrany zvnútra a ochrana zdrojov nakonfigurovaného doménového radiča.

Základné zabezpečenie doménového radiča zvnútra:

- Povolenie vzdialeného prístupu len administrátorovi (aby nemali možnosť prihlásenia sa do neho bežní užívatelia)
- Nedovoliť doménovému radiču používanie prehliadača
- Zabezpečenie jeho bezpečného umiestnenia v uzamykateľnom racku

Tieto nastavenia dokumentované nebudú, jedná sa o pomerne jednoduché nastavenia, ktoré zvládne aj laik a okrem toho posledné nastavenie nie je dôležité, keďže sa nejedná o reálnu prevádzku.

Z praktického hľadiska je však dôležité pre túto diplomovú prácu práve zabezpečenie zdrojov. Doménový radič je vo firemnom prostredí zdroj prostriedkov a svojim spôsobom databáza užívateľov, počítačov, nastavení, politík, dokumentov atp. Nie každý však môže mať k daným zdrojom prístup – toto delegujú bezpečnostné skupiny, ktoré presne definujú, kam môžu užívatelia danej skupiny pristupovať a čo všetko tam môžu robiť. Bezpečnostné politiky sú zas pravidlá, ktoré sa vzťahujú buď k zariadeniam, alebo užívateľom. Tieto pravidlá môžu byť rôzneho typu a ich konfigurácia môže prebiehať inak – niektoré politiky stačí len povoliť, u niektorých definovať skupiny, pre ktoré budú platiť a u niektorých je potrebné definovať napríklad cestu k zdroju.

V tejto diplomovej práci je doménový radič nakonfigurovaný tak, že má dva typy úložiska pre užívateľov, jedno je osobné a druhé je zdieľané. U osobného úložiska je dôležité, aby nemohlo, byť spolu zdieľané viacerými užívateľmi, čo bolo koniec koncov v predošlých kapitolách nakonfigurované. Zdieľaný disk „Z“ bol síce v predošlých kapitolách vytvorený a bolo nastavené jeho zdieľanie so skupinou „Users“, avšak je potrebné pomocou skupín delegovať, kam pracovníci môžu a nemôžu ísť a aké tam majú právomoci.

5.4.1 Nastavenie bezpečnostných skupín

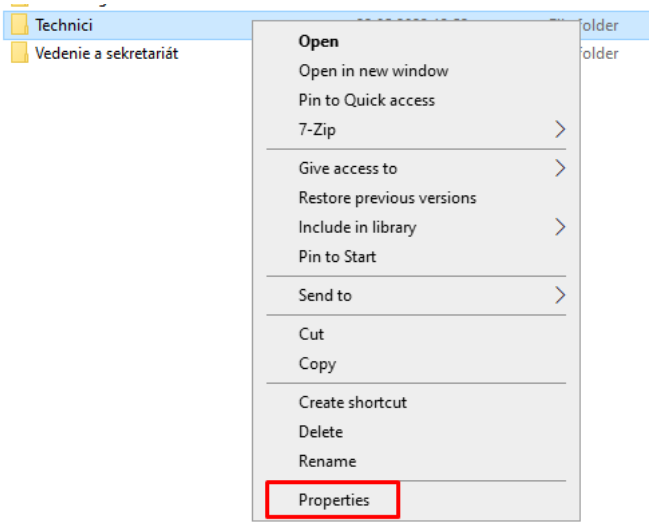
Ako bolo spomenuté v predošlej kapitole, skupiny definujú kam môžu užívatelia pristupovať a čo tam všetko môžu robiť. V tejto diplomovej práci bude nastavenie predvedené formou príkladu, ktorý sa neskôr bude testovať. Tento príklad sa priamo vzťahuje k zdieľanému disku „Z“, kde už sú vytvorené zložky pre jednotlivé oddelenia.

Náhodne boli vybrané skupiny „Pracovníci technického oddelenia“ a „Elektrikári“. Do skupiny „Pracovníci technického oddelenia“ spadajú všetci pracovníci (bez ohľadu na profesiu) a do skupiny „Elektrikári“ boli náhodne vybraní užívatelia Tadeáš Janík a Ivan Tvrdý. Tadeáš Janík je elektrikár na senior úrovni, Ivan Tvrdý je elektrikár na junior úrovni.

Pre nich je na zdieľanom disku „Z:“ vytvorená zložka elektrikári, ktorá sa delí na dve zložky – „Senior“ a „Junior“, kde si môžu ukladať pracovné veci, ktoré môžu spolu zdieľať. Nie je však vhodné, aby mal elektrikár na pozícii juniora prístup do zložky seniora. Takisto nie je vhodné, aby mal niekto z iného oddelenia prístup k ich spoločnej zložke a naopak – to bude v nasledujúcich krokoch konfigurované.

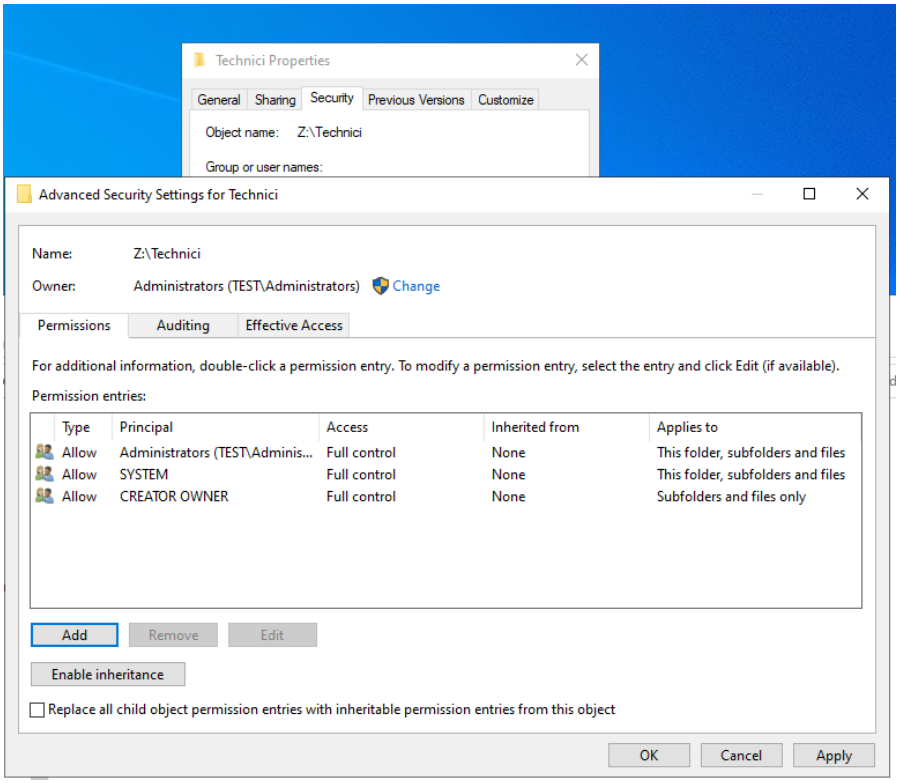
Momentálne je disk „Z:“ v stave, že je zdieľaný, ale editovať ho môže len administrátor.

Ďalej bude postup pokračovať len pre vybrané skupiny, u ostatných sa nakonfigurujú podobným spôsobom.



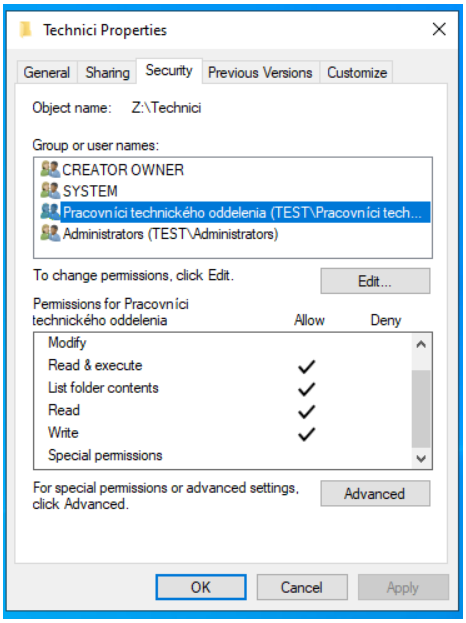
Obrázok 153 : Vlastnosti zložky „Technici“ (vlastný zdroj)

Prvým krok je v záložke „Security“ nájsť možnosť „Advanced“, kde bude potrebné vypnúť dedenie a vymazať nepotrebné skupiny.



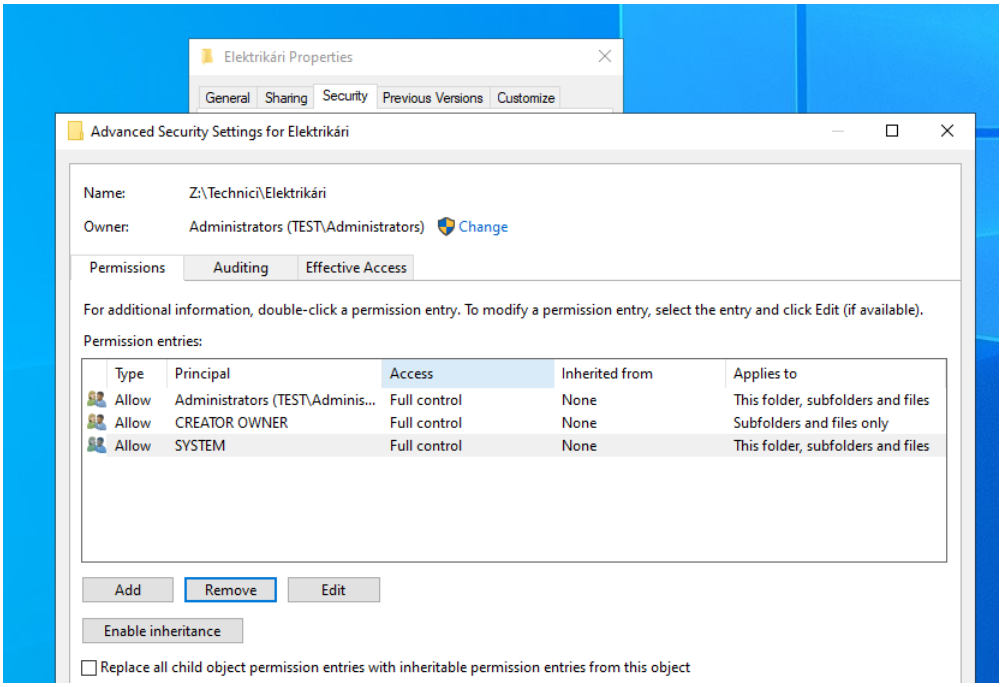
Obrázok 154 : Vypnutie dedenia a zmazanie nepotrebných skupín (vlastný zdroj)

Druhým krokom je umožniť prístup skupine „Pracovníci technického oddelenia“ a nastaviť im základné oprávnenia (teda nie plný prístup).



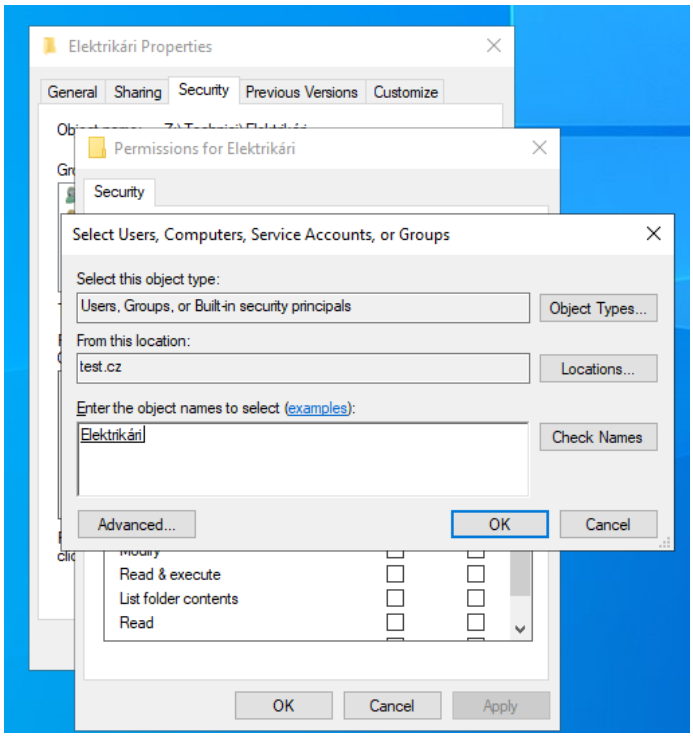
Obrázok 155 : Umožnenie prístupu a pridelenie práv pre skupinu „Technici“ (vlastný zdroj)

Pokračuje sa tým, že sa opäť vypne dedenie a zmažú sa nepotrebné skupiny, ale tentokrát pre zložku „Elektrikári“, ktorá je pod zložkou „Technici“.



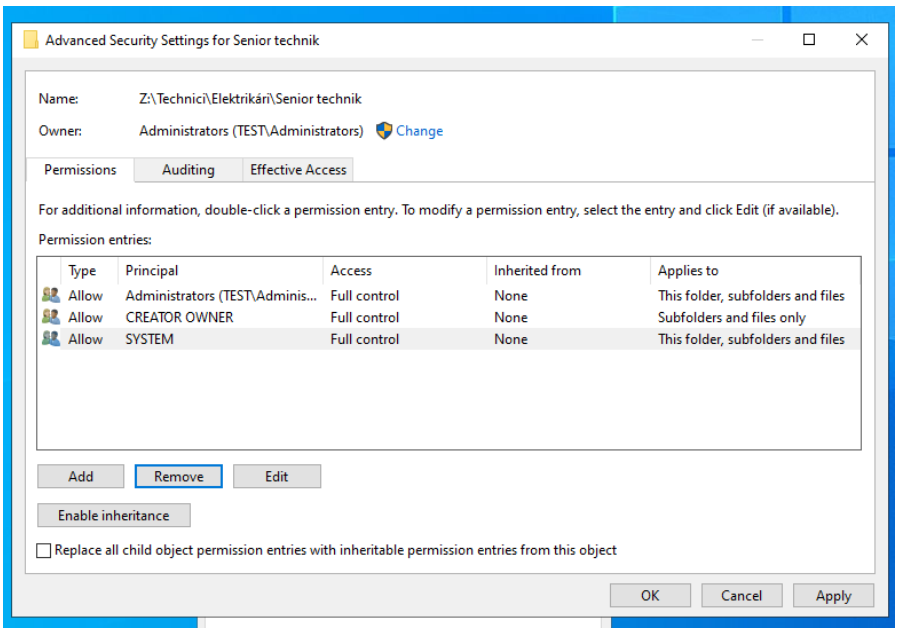
Obrázok 156 : Vypnutie dedenia a zmazanie nepotrebných skupín pre zložku „Elektrikári“

Nasleduje pridelenie prístupu a základných oprávnení pre skupinu „Elektrikári“.



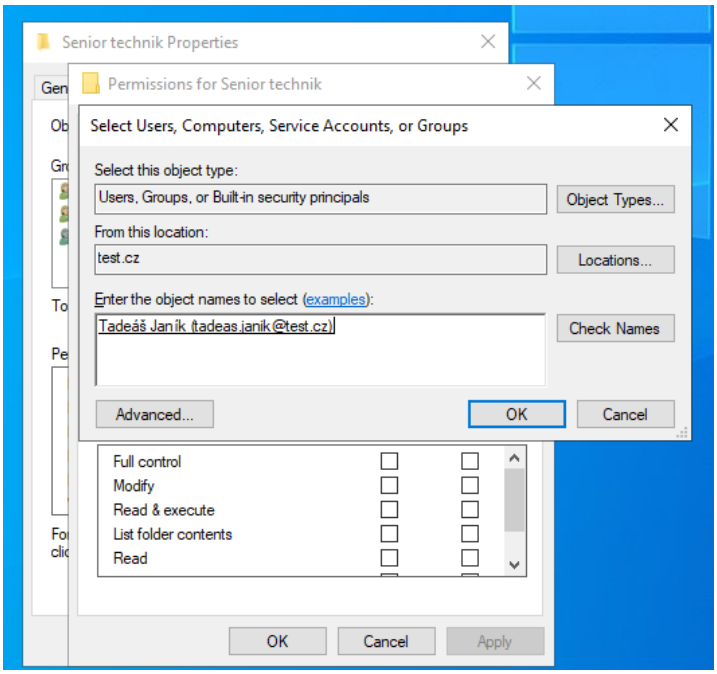
Obrázok 157 : Umožnenie prístupu a pridelenie práv pre skupinu „Technici“ (vlastný zdroj)

Nasleduje predposledný krok, v ktorom sa vypne dedenie a zmažú sa nepotrebné skupiny pre zložku „Senior technik“.



Obrázok 158 : Vypnutie dedenia a zmazanie nepotrebných skupín pre zložku „Senior technik“ (vlastný zdroj)

Finálnym krokom je nastavenie prístupu a základných oprávnení do zložky „Senior technik“ Tadeášovi Janíkovi.



Obrázok 159 : Umožnenie prístupu a základných oprávnení Tadeášovi Janíkovi (vlastný zdroj)

5.4.2 Konfigurácia skupinových politík

Poslednou časťou konfigurácie doménového radiča pred testovaním je nastavenie skupinových politík.

Doménový radič je server, ktorý potrebuje byť „šitý na mieru“ pre danú organizáciu, a to isté sa vzťahuje aj ku skupinovým politikám.

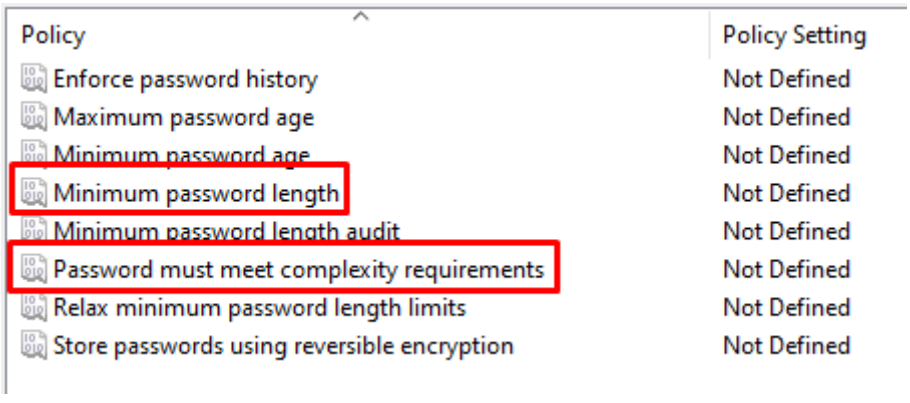
Nastavenie skupinových politík závisí teda na dohode celej organizácie, alebo lepšie povedané hlavných vedúcich – ide najmä o to, ako veľmi budú prísne. Politiky sú veľmi mocným nástrojom, pomocou ktorých je možné nastaviť nespočetné množstvo parametrov, pre túto diplomovú prácu boli ako príklad vybrané tri politiky, ktoré sa bežne konfigurujú.

Ako príklad budú najprv nastavované skupinové politiky, ktoré sa viažu pre počítače, teda pre OU „Počítače a notebooky“ a následne skupinové politiky pre OU „Vedenie a sekretariát“ (teda pre užívateľov v tejto OU).

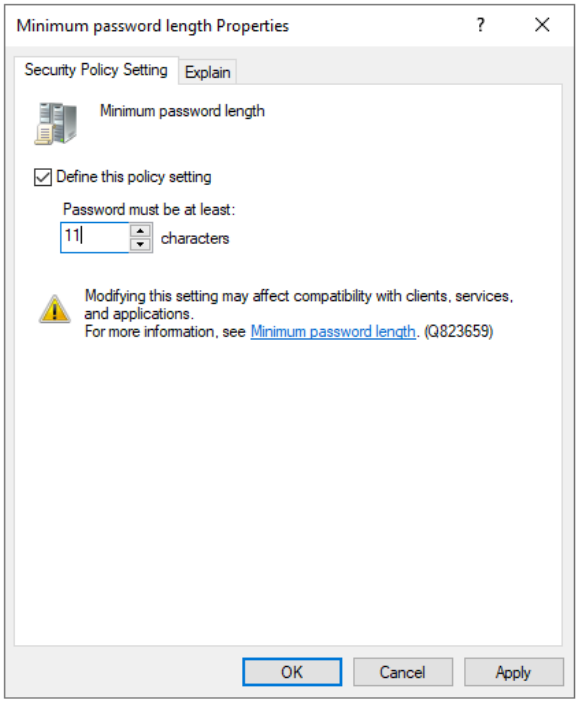
Politiky pre OU „Počítače a notebooky“:

Prvým krokom je vytvorenie GPO pre OU „Počítače a notebooky“ s názvom „Všeobecné“. Tento krok sa vyskytuje v praktickej časti niekoľkokrát, preto bude jeho úvod vynechaný.

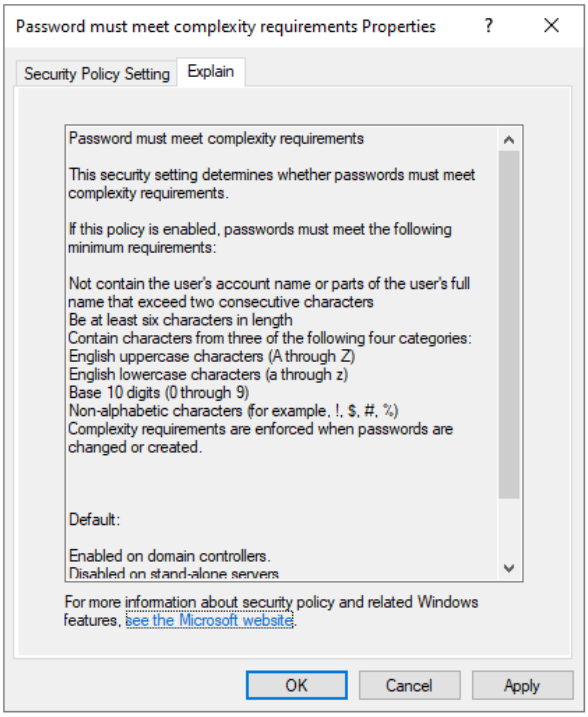
Ako prvé budú nastavené politiky pre heslá „Minimum password length“ a „Password must meet complexity requirements“. Tieto politiky definujú požiadavky na heslá.



Obrázok 160 : Vybrané politiky pre heslá (vlastný zdroj)

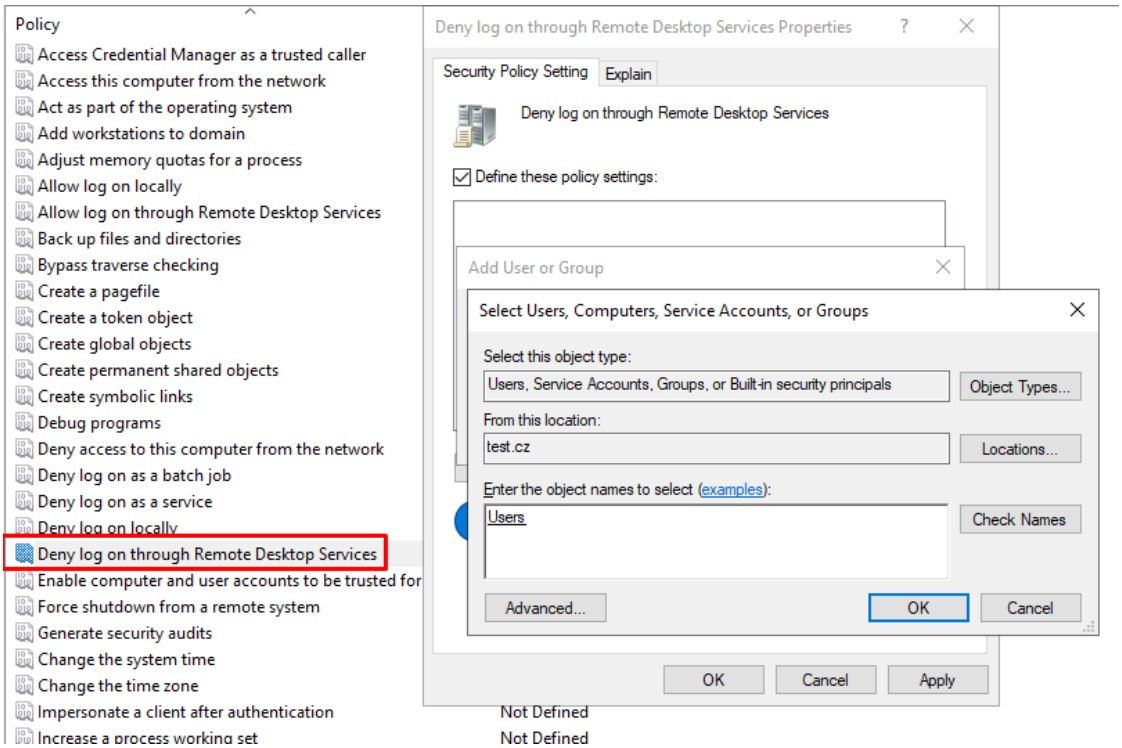


Obrázok 161 : Nastavenie politiky „Minimum password length“ (vlastný zdroj)



Obrázok 162 : Definícia politiky „Password must meet complexity requirements“ (vlastný zdroj)

Poslednou politikou, ktorá bude nastavovaná je „Deny log on through Remote Desktop Services“. Táto politika znemožňuje pristupovať na vzdialené plochy. Nastavená bude pre skupinu „Users“.

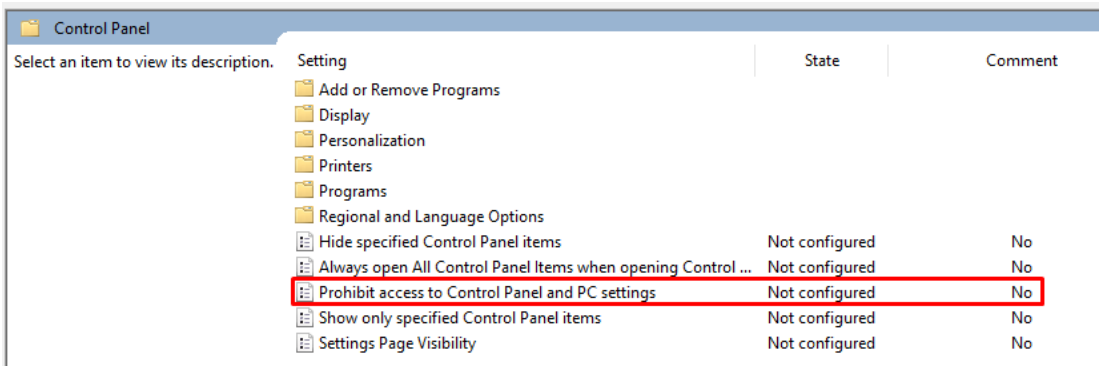


Obrázok 163 : Nastavenie politiky „Deny log on through Remote Desktop Services „(vlastný zdroj)

Politiky pre OU „Vedenie a sekretariát“:

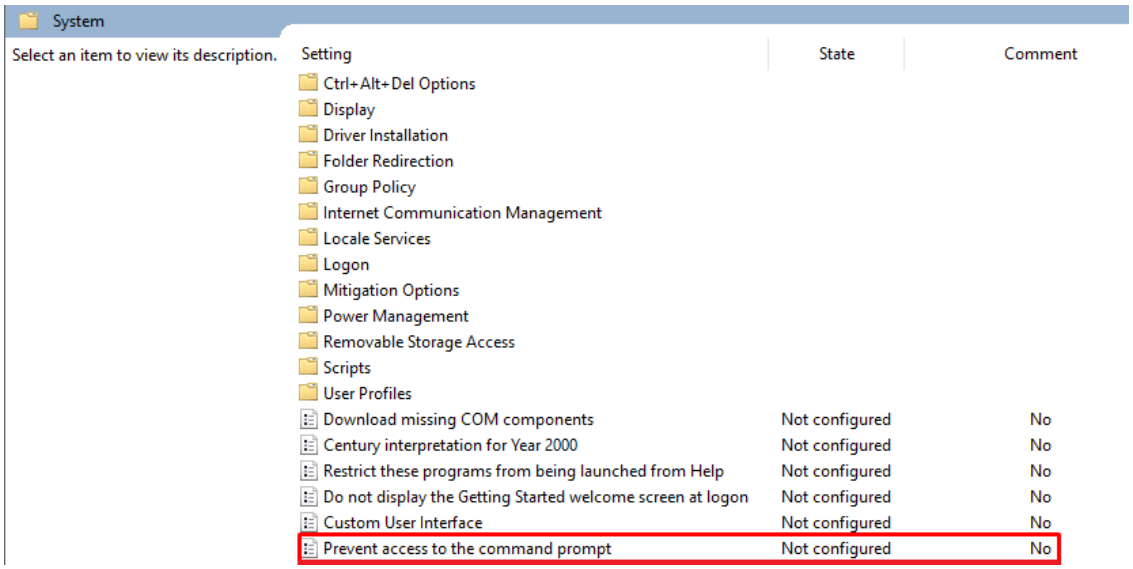
Prvým krokom je vytvorenie GPO pre OU „Vedenie a sekretariát“ s názvom „Všeobecné“. Tento krok sa vyskytuje v praktickej časti niekoľkokrát, preto bude jeho úvod vynechaný.

Ako prvá politika bude nastavená „Prohibit access to Control Panel and PC settings“, táto politika zabraňuje prístupu k ovládaciemu panelu a počítačovým nastaveniam. Túto politiku stačí len zapnúť.



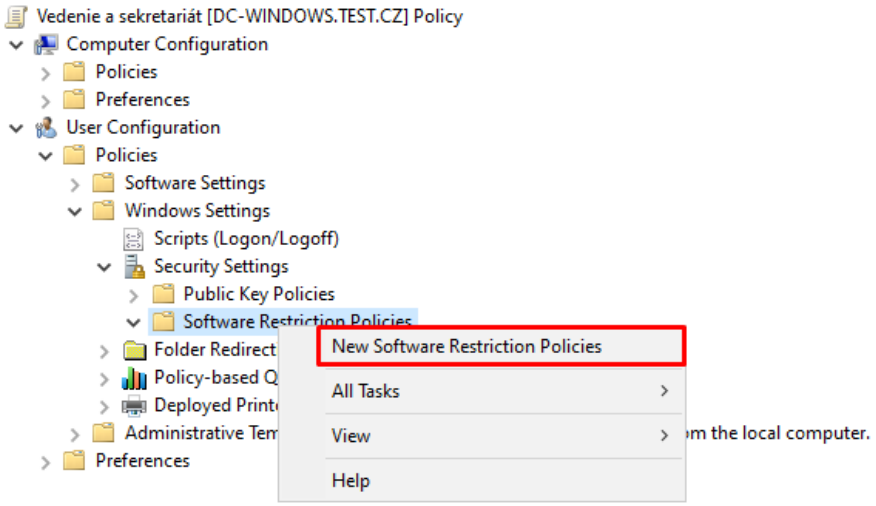
Obrázok 164 : Výber politiky „Prohibit access to Control Panel and PC settings„ (vlastný zdroj)

Ako druhá politika bude nastavená „Prevent access to the command prompt“. Táto politika zabraňuje prístupu k príkazovému riadku. Opäť, politiku stačí len zapnúť.



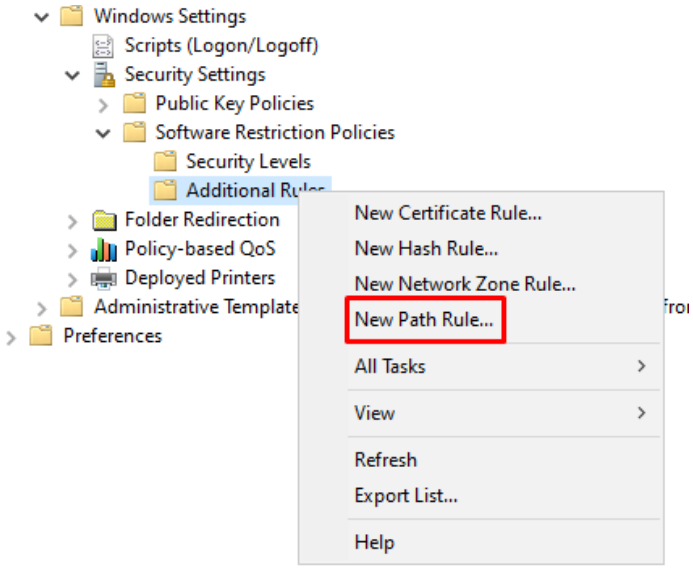
Obrázok 165 : Výber politiky „Prevent access to the command prompt„ (vlastný zdroj)

Ako posledná bude nastavená politika, ktorá zabraňuje prístupu k powershellu. Táto politika sa nenachádza medzi preddefinovanými politikami, je potrebné ju vytvoriť. Túto možnosť poskytujú „Software Restriction Policies“

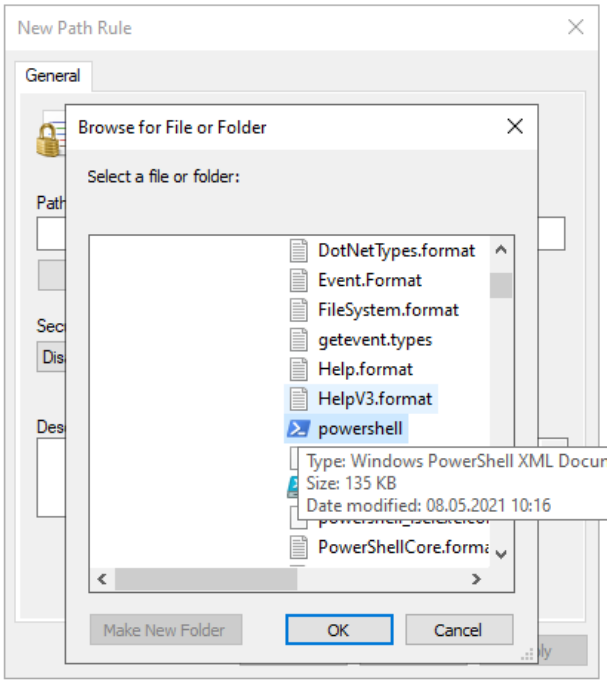


Obrázok 166 : Vytvorenie novej politiky pre zákaz prístupu k powershell

Následne je potrebné definovať cestu k software, ktorý sa nemá spúšťať. V zozname je ho potrebné nájsť, powershell sa nachádza v systémových zložkách.



Obrázok 167 : Vytvorenie novej politiky pre zákaz prístupu k powershell



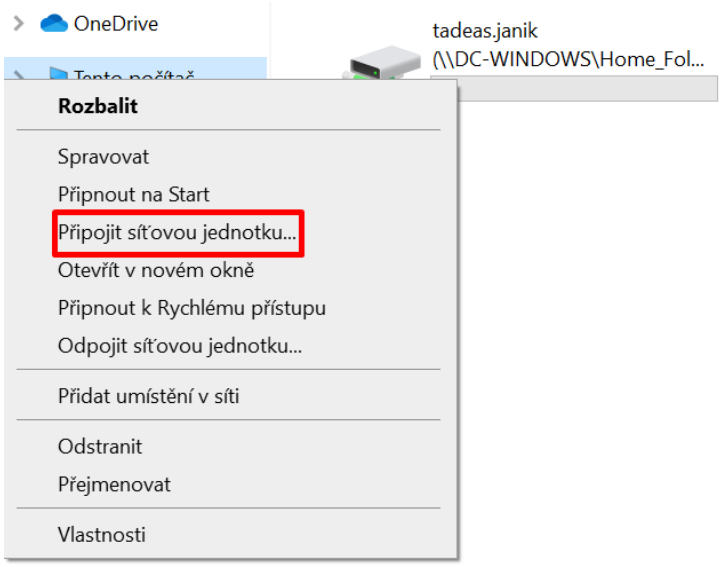
Obrázok 168 : Definovanie cesty k software (vlastný zdroj)

5.4.3 Testovanie nastavení skupín a politík

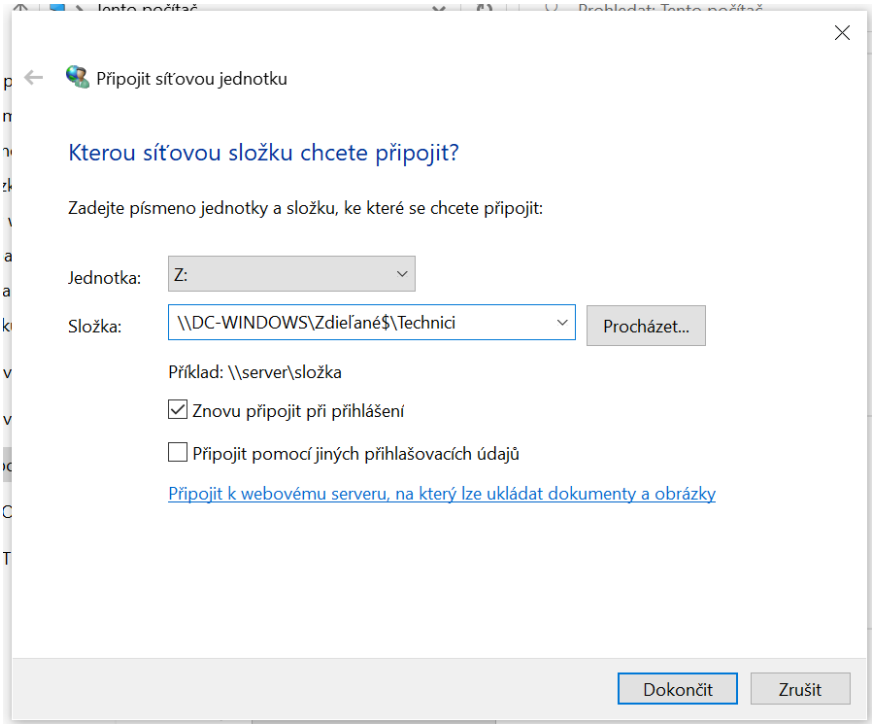
Všetky výsledky predošlej konfigurácie skupín a politík vyšli pozitívne.

Najprv prebehlo prihlásenie na účet Tadeáša Janíka, odkiaľ boli testované prístupy do zložky cudzieho oddelenia a do zložky, kam má mať prístup len on.

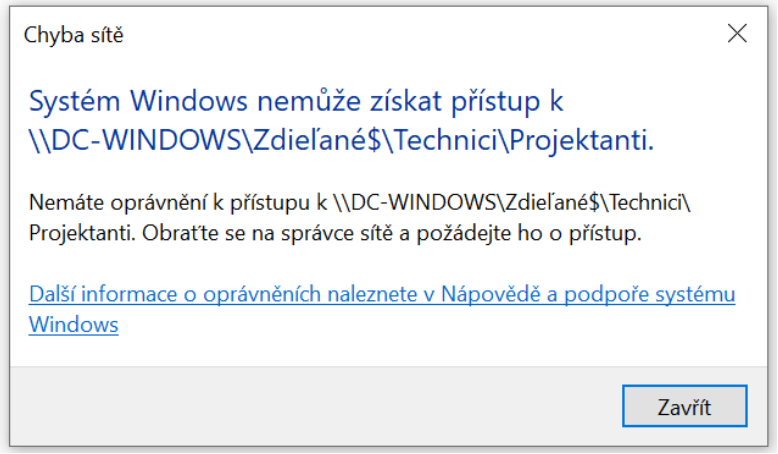
Tomu predchádzalo pripojenie sieťovej zložky.



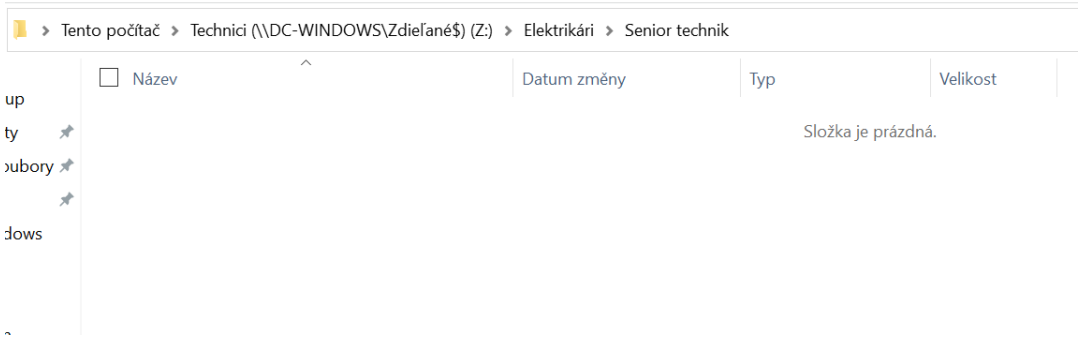
Obrázok 169 : Pripojenie sieťovej jednotky pre užívateľa „Tadeáš Janík“ (vlastný zdroj)



Obrázok 170 : Zadanie cesty pre prístup do zložky „Technici“ (vlastný zdroj)

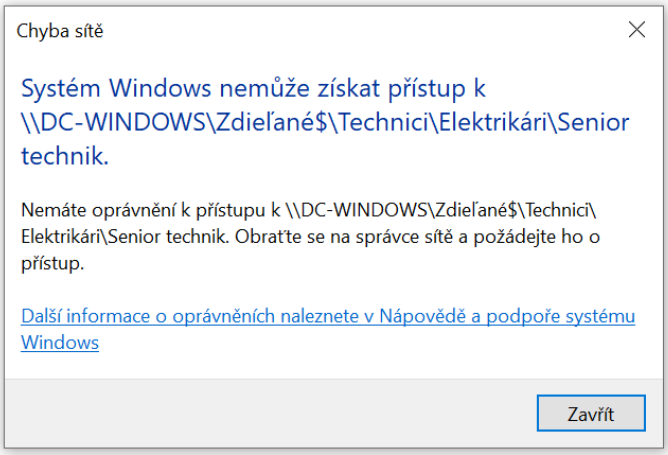


Obrázok 171 : Užívateľ „Tadeáš Janík“ nemôže pristúpiť k náhodnej zložke iného oddelenia (vlastný zdroj)



Obrázok 172 : Užívateľ „Tadeáš Janík“ môže pristúpiť do zložky, kam má mať prístup len on (vlastný zdroj)

Ďalším krokom bolo otestovať, či sa dostane elektrikár na junior pozícii do zložky seniorného technika. Účty sa teda vymenili a nastalo prihlásenie užívateľa „Ivan Tvrdý“ a mapovanie zložky, ako to bolo v prípade užívateľa Tadeáša Janíka.



Obrázok 173 : Užívateľ „Ivan Tvrdý“ sa nedostane do zložky seniorných technikov (vlastný zdroj)

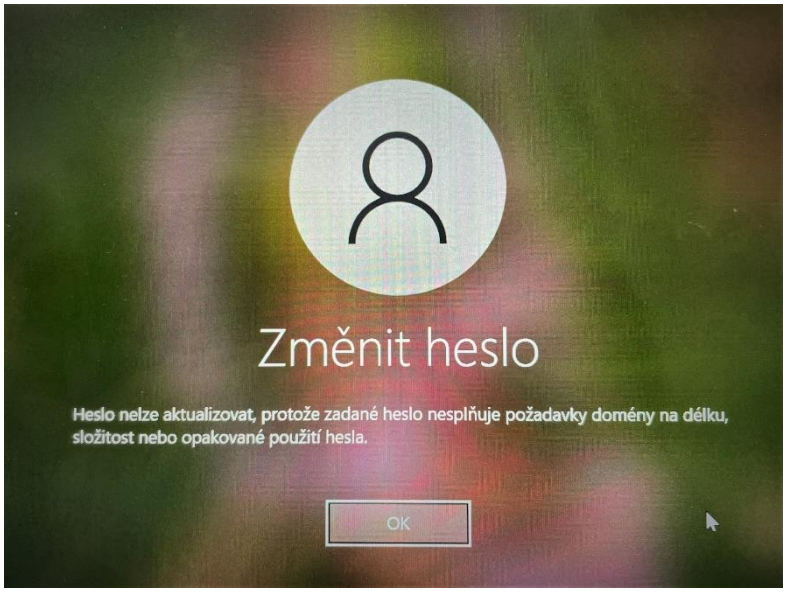
Následne sa účet znova prepol na účet z OU „Vedenie a sekretariát“ „Tatiana Kováčová“. Cieľom bolo otestovať na ňom nastavené politiky (tento účet bol vybraný preto, pretože politiky pre užívateľov boli nastavované na OU „Vedenie a sekretariát“, nie na všetky ostatné OU).

Testované boli všetky politiky z predošlej kapitoly.

Pre počítače to boli politiky: „Minimum password length“ , „Password must meet complexity requirements“ a „Deny log on through Remote Desktop Services„.

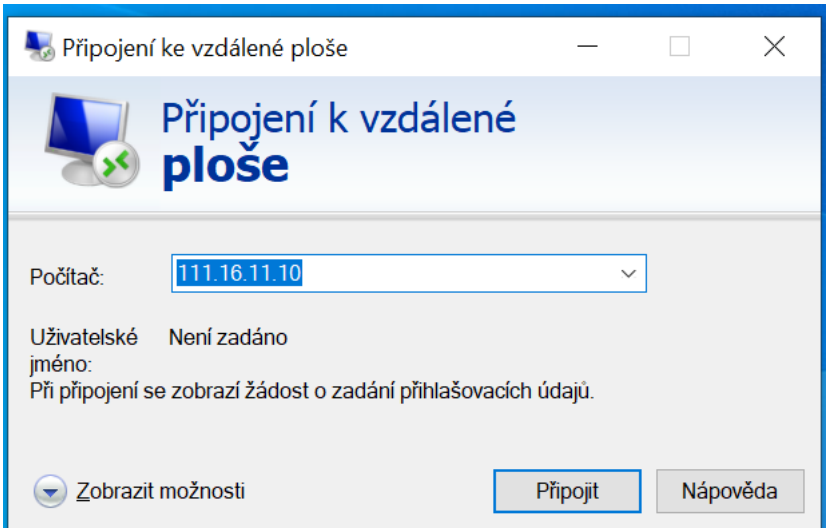
Pre užívateľov to boli politiky: „Prohibit access to Control Panel and PC settings“ , „Prevent access to the command prompt“ a samostatná politika pre zákaz prístupu k powershell.

Po nesplnení požiadavkov na heslo nie je možná jeho zmena.

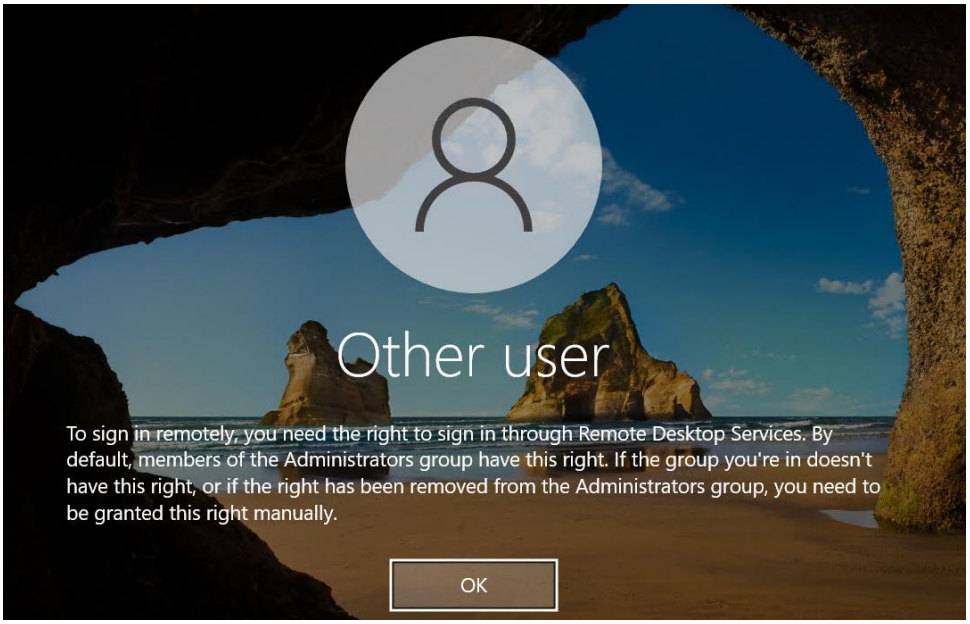


Obrázok 174 : Nemožná zmena hesla (vlastný zdroj)

Medzitým sa na radiči nastavil prístup pre účet „Tatiana Kováčová“, aby bolo možné testovať politiku zákazu RDS.

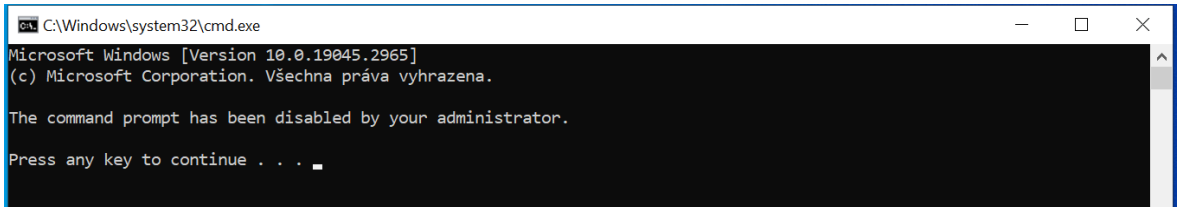


Obrázok 175 : Zadanie IP adresy radiča (vlastný zdroj)



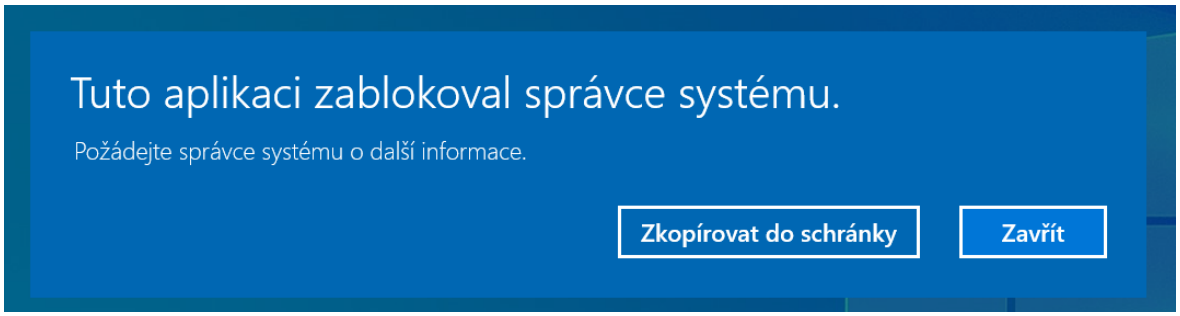
Obrázok 176 : Nie je možný prístup na radič (vlastný zdroj)

Prístup k CMD možný nie je, nastavenia sa nedajú ani zapnúť (možno je škoda, že nevybehne nejaká chybová hláška, takto to vyzerá, že neustále padajú, ale v skutočnosti to robí nastavenie politiky).



Obrázok 177 : Nie je možný prístup k CMD (vlastný zdroj)

To isté platí aj pre powershell, ktorý takisto nie je dostupný.



Obrázok 178 : Nie je možný prístup k powershell (vlastný zdroj)

Testy teda prebehli úspešne, týmto je možné konfiguráciu Windows DC uzavrieť a presunúť sa na druhú časť praktickej časti, ktorá je vďaka veľmi podobnej konfigurácii znateľne kratšia – to jej však neuberá na kvalite, nie je však potrebné tie isté kroky dokumentovať zdvojene.

6 PRÍPRAVA DOMÉNOVÉHO RADIČA – SYSTÉM LINUX

Táto kapitola bude svojim spôsobom rozdielna od kapitoly inštalácie a konfigurácie doménového radiča na systéme Windows.

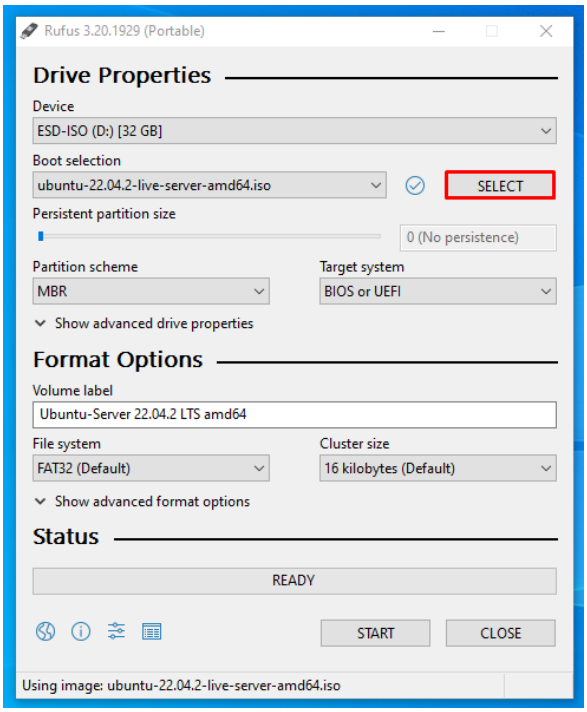
Linuxové doménové radiče nie sú vôbec bežné, skôr sa serverové distribúcie Linuxu využívajú na iné účely – napríklad: VPN server, Webserver, SQL server, aplikačný server atď.

Systém Linux server sám o sebe nebol navrhnutý na to, aby bol doménovým radičom – v tomto má výrazne napred systém Windows, ktorý vyvíja priamo software pre doménové radiče. Linux je však otvorený systém, ktorý sa neustále vyvíja a čím ďalej, tým lepšie sa integruje s ostatnými systémami. Systém linux server sa ale dá nakonfigurovať tak, aby bol doménovým radičom, avšak musí pre to využiť službu samba a nástroje Microsoftu.

6.1 Inštalácia operačného systému Linux Ubuntu Server 22.04.2 LTS

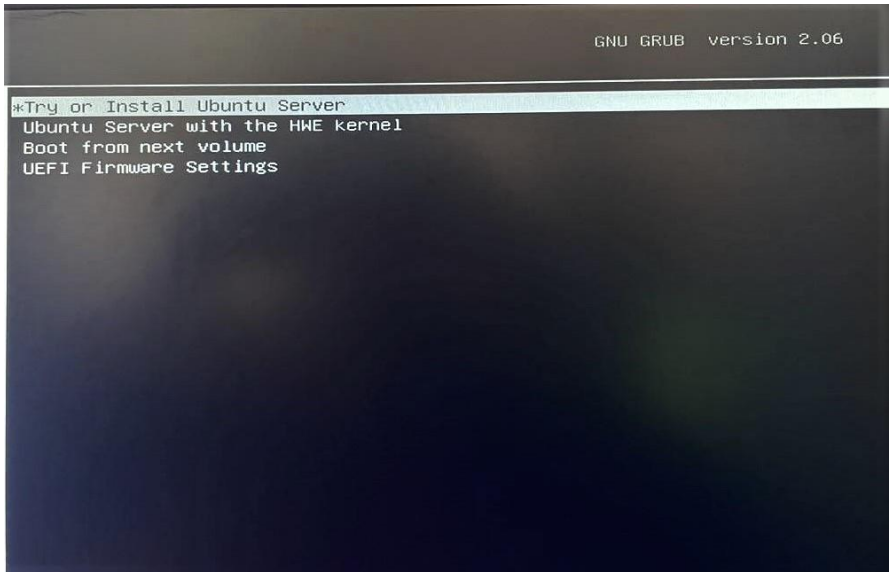
Inštalácia operačného systému Linux nie je vôbec zložitá – nebude potrebná ani žiadna licencia, keďže sa jedná o otvorený systém. Linux sa dá stiahnuť priamo z ich oficiálnych stránok, pre túto diplomovú prácu bol zvolený OS verzie 22.04.02 – teda Jammy Jellyfish.

Pred inštaláciou si je potrebné tak, ako v prípade Windowsu pripraviť inštalačné USB pomocou software Rufus.



Obrázok 179 : Príprava inštalačného USB(vlastný zdroj)

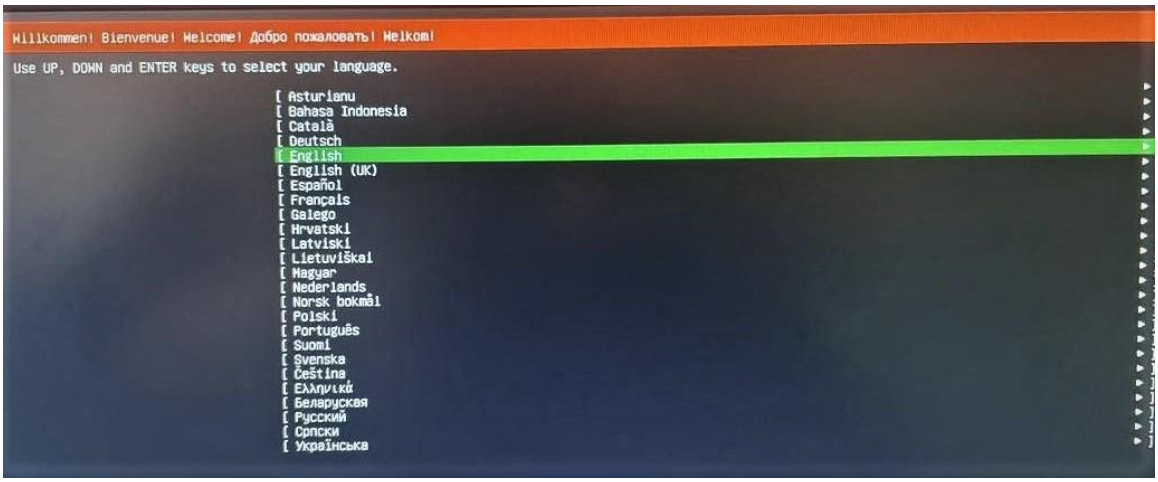
Po vložení inštalačného USB do počítača započne samotná inštalácia. Hneď na úvod sa sprievodca pýta, čo sa bude inštalovať / spúšťať, zvolená je možnosť inštalácie systému.



Obrázok 180 : Zvolenie inštalácie systému (vlastný zdroj)

Následne sprievodca pokračuje k možnostiam výberu jazyka – vybraná bola angličtina.

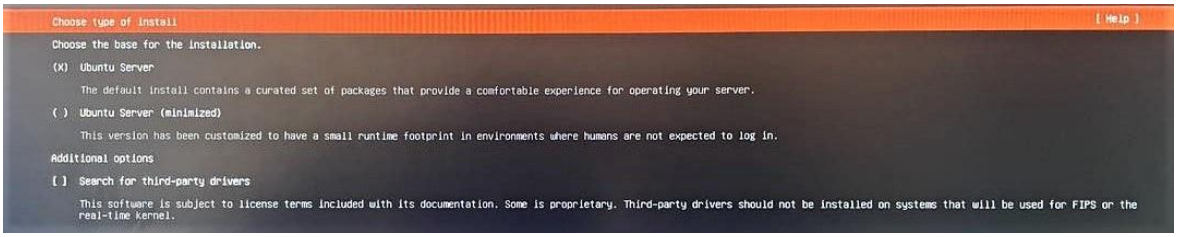
Ďalej je možnosť nastaviť si klávesnicu, ponechaná bude len anglická.



Obrázok 181 : Výber jazyka (vlastný zdroj)

Obrázok 182 : Nastavenie klávesnice (vlastný zdroj)

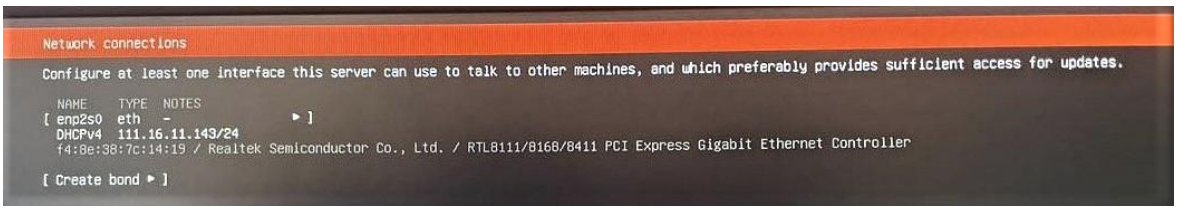
V ďalšom kroku dáva sprievodca na výber, aký základ sa má nainštalovať – vybraná bola možnosť „Ubuntu Server“.



Obrázok 183 : Výber základu inštalácie (vlastný zdroj)

Pred nasledujúcim krokom je potrebné na routri zapnúť službu DHCP, aby pridelila zariadeniam adresy.

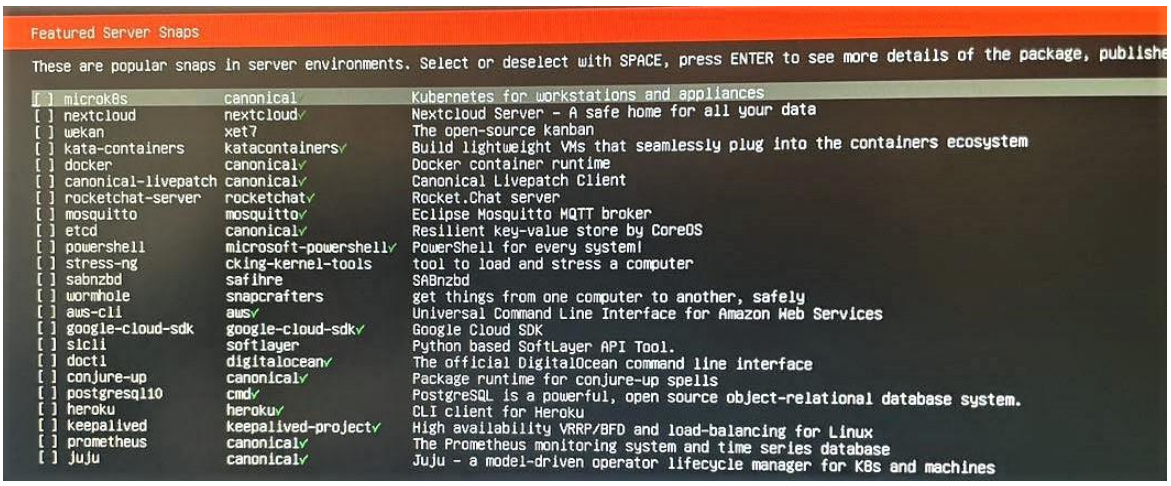
Následne je potrebné nastaviť sieťové rozhranie, aby mohla inštalácia plne prebehnúť. Toto zariadenie je pripojené k internetu prostredníctvom kábla, takže dôjde k automatickej detekcii rozhrania.



Obrázok 184 : Detekcia sieťového rozhrania (vlastný zdroj)

Ďalší krok dáva možnosť konfigurácie proxy – tá využívaná nie je, takže sa môže preskočiť.

Ďalším krokom je výber súčastí, ktoré sa majú nainštalovať spolu s operačným systémom – z uvedených bol vybraný iba powershell, ostatné sa dajú vždy doinštalovať.

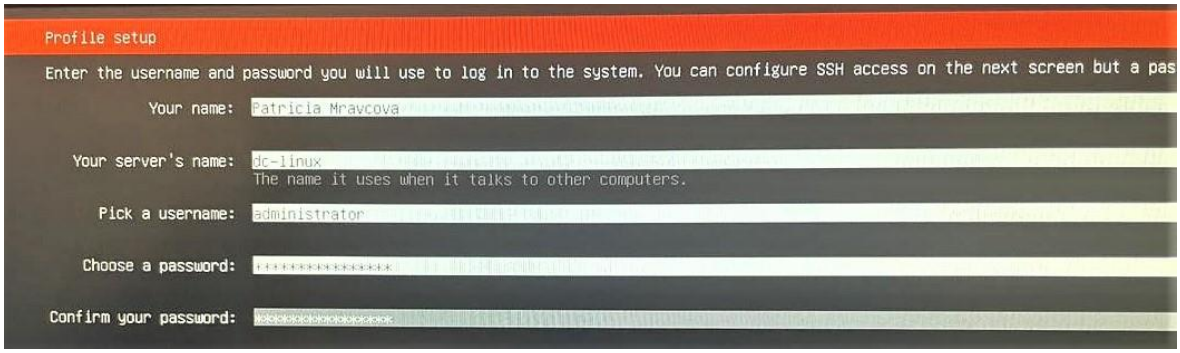


Obrázok 185 : Výber súčastí (vlastný zdroj)

Potom sprievodca dáva možnosť inštalácie OpenSSH pre vzdialený prístup – ten sa hodí vždy.

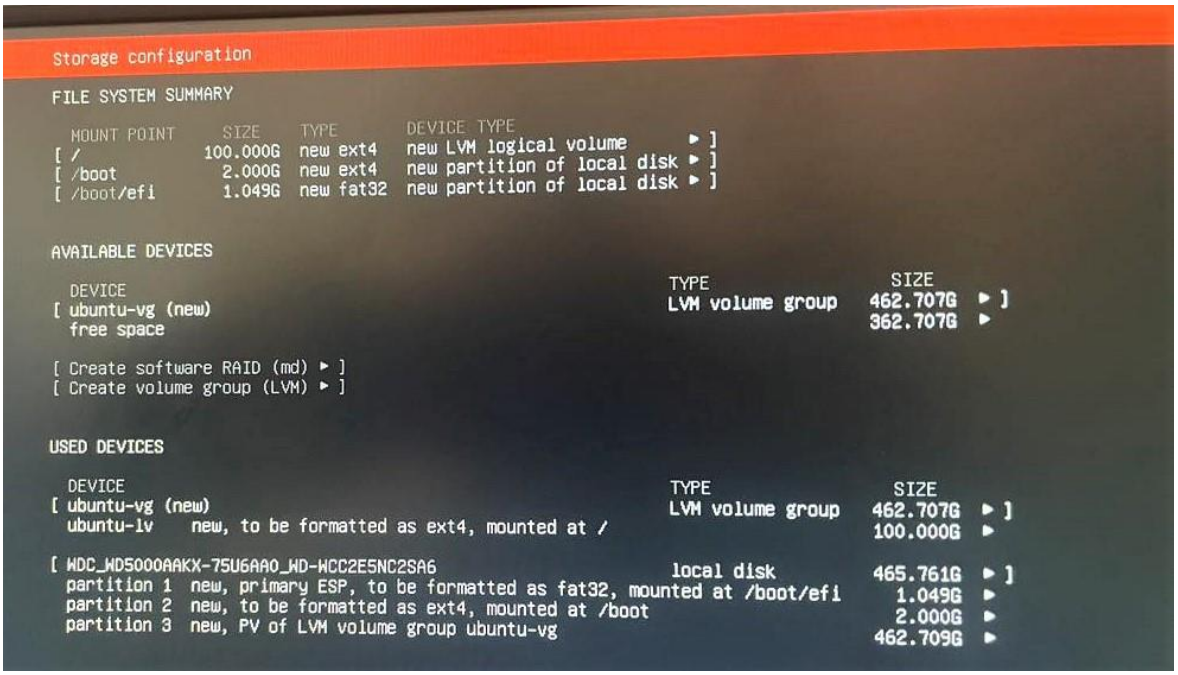
Obrázok 186 : Možnosť inštalácie OpenSSH (vlastný zdroj)

Ďalším krokom je základné nastavenie profilu – čiže výber mena, hostname servera, užívateľské meno a heslo.



Obrázok 187 : Nastavenie profilu (vlastný zdroj)

Posledným krokom je nastavenie úložiska – v tomto prípade bude pre inštaláciu zvolený celý disk, nie je potrebné ho nijak deliť. Po tomto kroku nasleduje už len zhrnutie, po ktorom započne samotná inštalácia. Po inštalácii je potrebné zariadenie reštartovať a prihlásiť sa s nastaveným užívateľským menom a heslom.

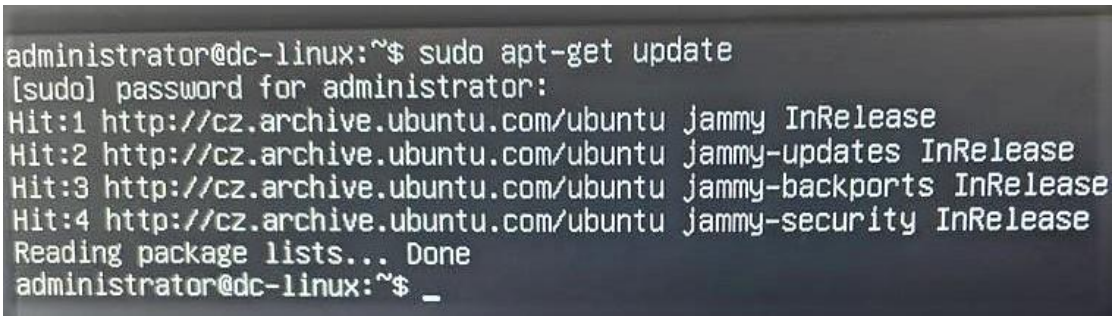


Obrázok 188 : Nastavenie úložného priestoru (vlastný zdroj)

6.2 Príprava počítača pred konfiguráciou samby

Pred samotnou konfiguráciou samby (ktorá zabezpečí transformáciu servera na doménový radič), je potrebných pár úprav.

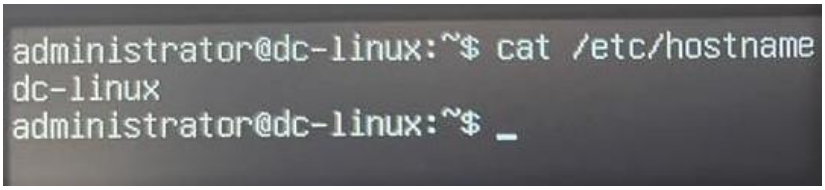
Hneď prvým krokom je aktualizácia OS – čiže update a upgrade. Systém nemá nainštalované grafické rozhranie, takže konfigurácia všetkých častí prebehne prostredníctvom príkazového riadku.



Obrázok 189 : Načítanie balíčkov (vlastný zdroj)

Obrázok 190 : Aktualizácia (vlastný zdroj)

Ďalším krokom nastavenie hostname – táto časť bola splnená už pri inštalácii operačného systému, takže bude len overené.



Obrázok 191 : Kontrola hostname (vlastný zdroj)

Teraz je potrebné serveru priradiť indentitu – čiže nastaviť hostname na IP adresu a nastaviť statickú IP adresu.

```
administrator@dc-linux:~$ sudo nano /etc/hosts_
```

Obrázok 192 : Cesta k editácii hosts (vlastný zdroj)

```
  GNU nano 6.2
127.0.0.1 localhost
111.16.11.20 dc-linux

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Obrázok 193 : Nastavenie IP adresy a hostname (vlastný zdroj)

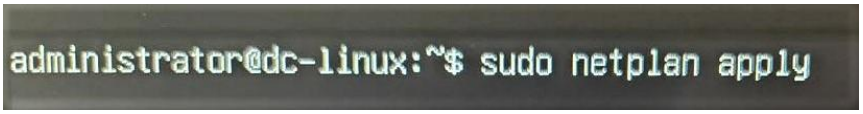
```
administrator@dc-linux:~$ sudo nano /etc/netplan/00-installer-config.yaml
```

Obrázok 194 : Cesta k editácii sieťových nastavení (vlastný zdroj)

```
  GNU nano 6.2
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp2s0:
      dhcp4: false
      addresses: [111.16.11.20/24]
      gateway4: 111.16.11.1
      nameservers:
        addresses: [111.16.11.20, 8.8.8.8]
  version: 2
```

Obrázok 195 : Nastavenie statickej IP adresy (vlastný zdroj)

Po nastavení je ešte potrebné prevedené zmeny aplikovať a následne zariadenie reštarovať.



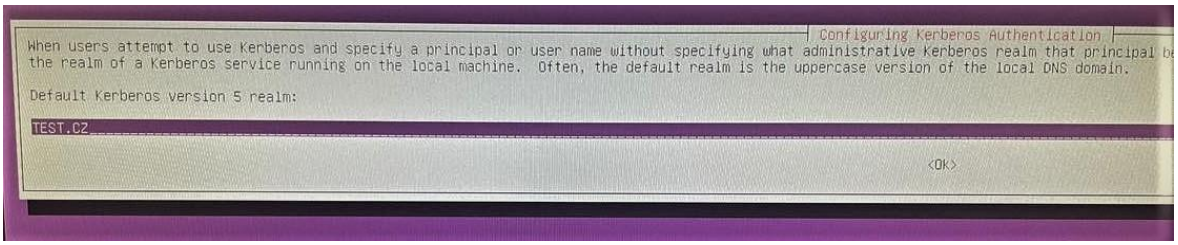
Obrázok 196 : Aplikovanie prevedených zmien (vlastný zdroj)

6.3 Konfigurácia samby a role DNS

Teraz môže finálne započať konfigurácia samby – čím sa zároveň nakonfigurujú aj role AD DS a DNS. Najprv je potrebné teda samotnú sambu a jej súčasti nainštalovať – potrebné sú: winbind (umožňuje WIN/LIN počítačom zdieľanie infomácií o užívateľoch a počítačoch), krb5-config (slúži pre autentifikáciu užívateľa), smbclient (pre zdieľanie súborov na sieti), dnsutils (pre testovanie DNS) a set sieťových nástrojov net-tools.

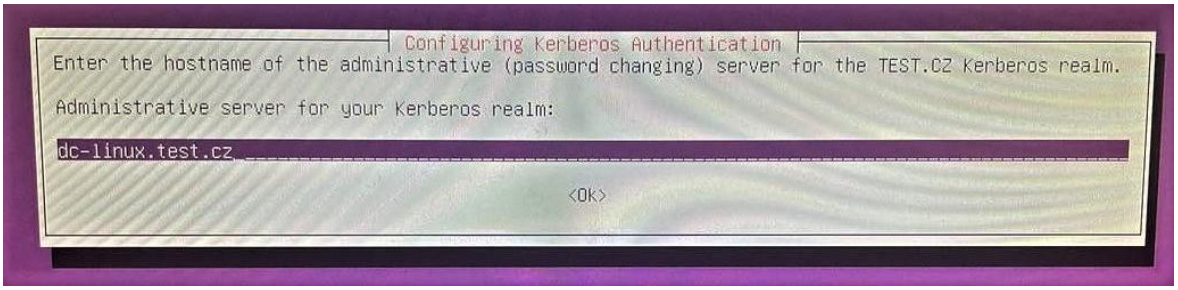
Obrázok 197 : Inštalácia samby a potrebných súčastí (vlastný zdroj)

Medzitým, čo prebieha inštalácia je potrebné nastaviť pár medzikrokov – tým prvým bude kerberos realm (doména, v ktorom je overovací server, ktorý má oprávnenie overovať užívateľov, hostiteľov a služby). Napísaný musí byť veľkými písmenami.



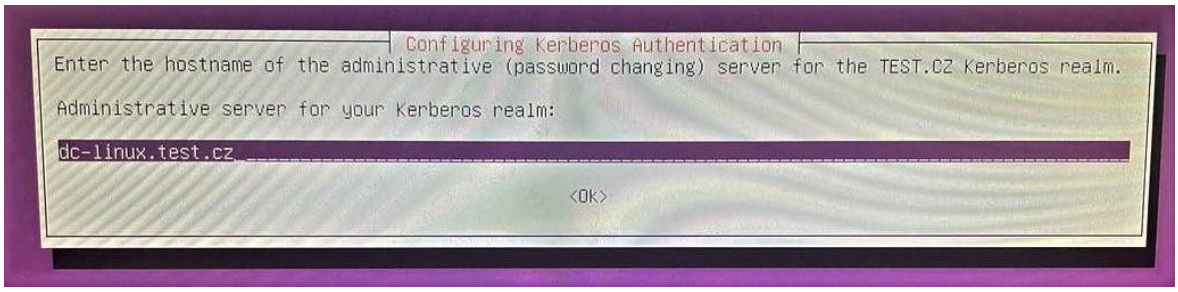
Obrázok 198 : Nastavenie realmu (vlastný zdroj)

Potom je potrebné nastaviť server pre realm – teda samotný overovací oprávnený server.



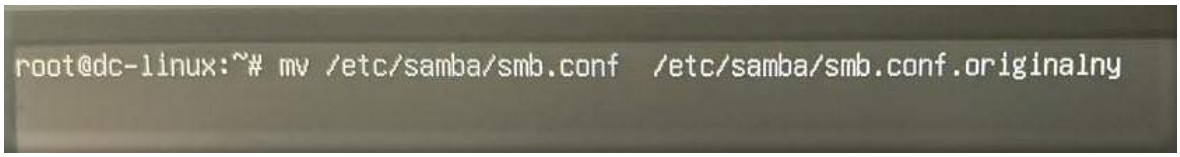
Obrázok 199 : Nastavenie overovacieho servera (vlastný zdroj)

Posledným medzikrokom je nastavenie administračného serveru pre realm (rovnaký, ako v predošlom kroku).



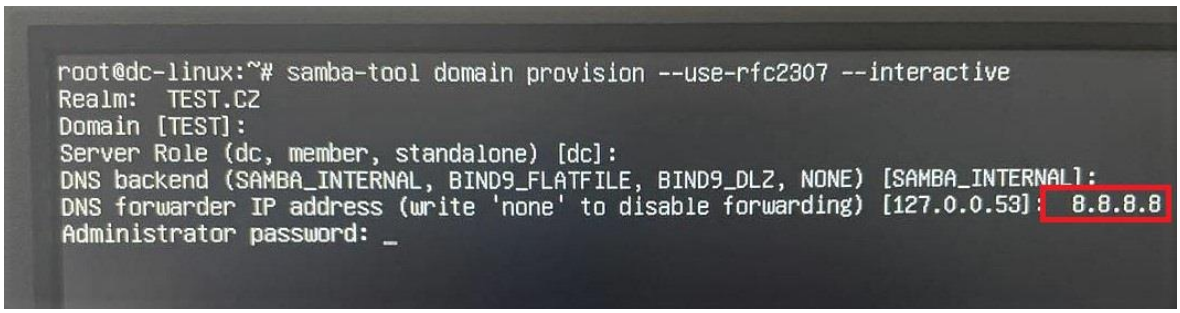
Obrázok 200 : Nastavenie administračného servera (vlastný zdroj)

Ďalší krok smeruje k zálohovaniu súboru smb.conf. Záloha sa pre testovacie zariadenie robiť nemusí, v reálnej prevádzke je však odporúčané vždy pred rekonfiguráciou zálohovať.



Obrázok 201 : Zálohovanie súboru smb.conf (vlastný zdroj)

Posledným krokom je nastavenie zaisťovania a nastavenie parametrov pre DNS server.

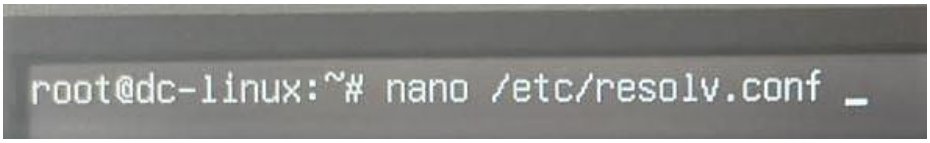


Obrázok 202 : Nastavenie zaisťovania a role DNS (vlastný zdroj)

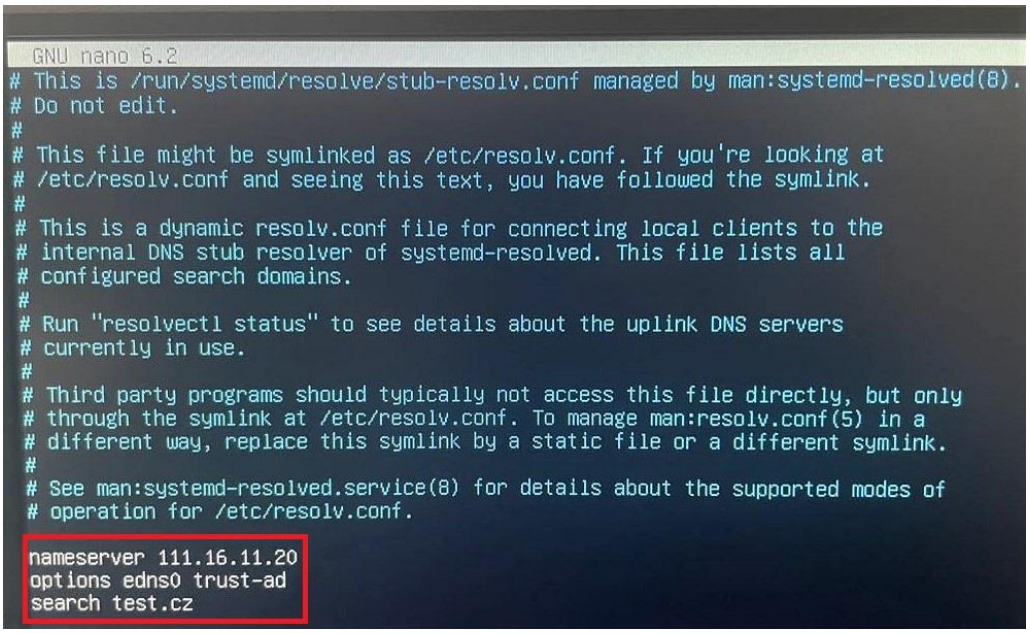
Nasleduje krok prekopírovania krb5.conf do /etc/.

Obrázok 203 : Prekopírovanie krb5.conf (vlastný zdroj)

Následne je potrebné upraviť súbor resolv.conf.

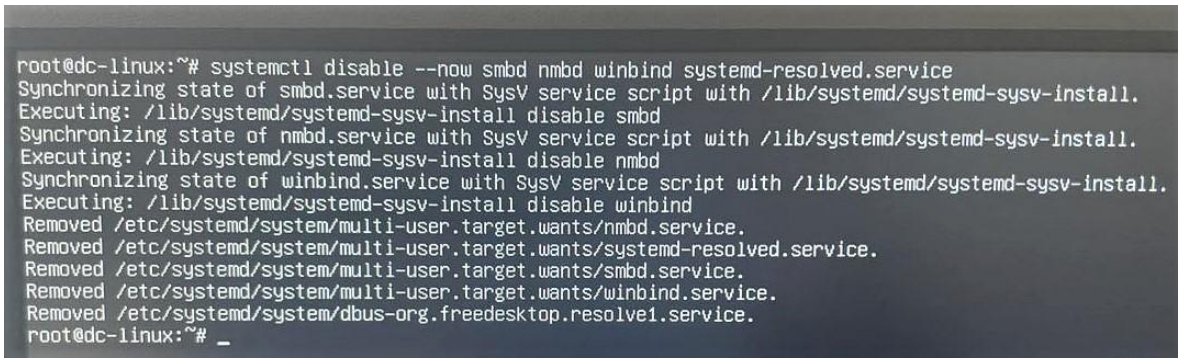


Obrázok 204 : Cesta k súboru resolv.conf (vlastný zdroj)



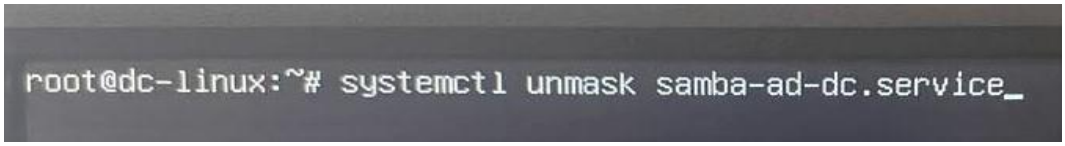
Obrázok 205 : Konfigurácia resolv.conf (vlastný zdroj)

Po tomto kroku je potrebné vypnúť služby, ktoré nie sú potrebné.



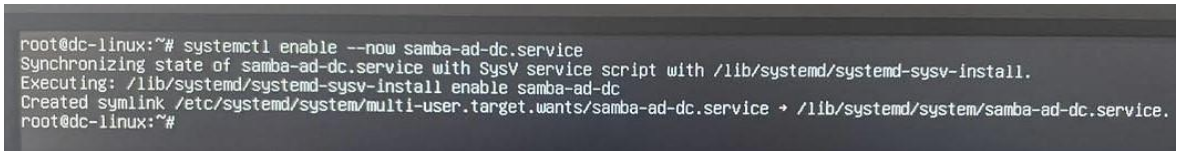
Obrázok 206 : Vypnutie nepotrebných služieb (vlastný zdroj)

Nasledujúci krok odmaskuje služby Samba Directory.



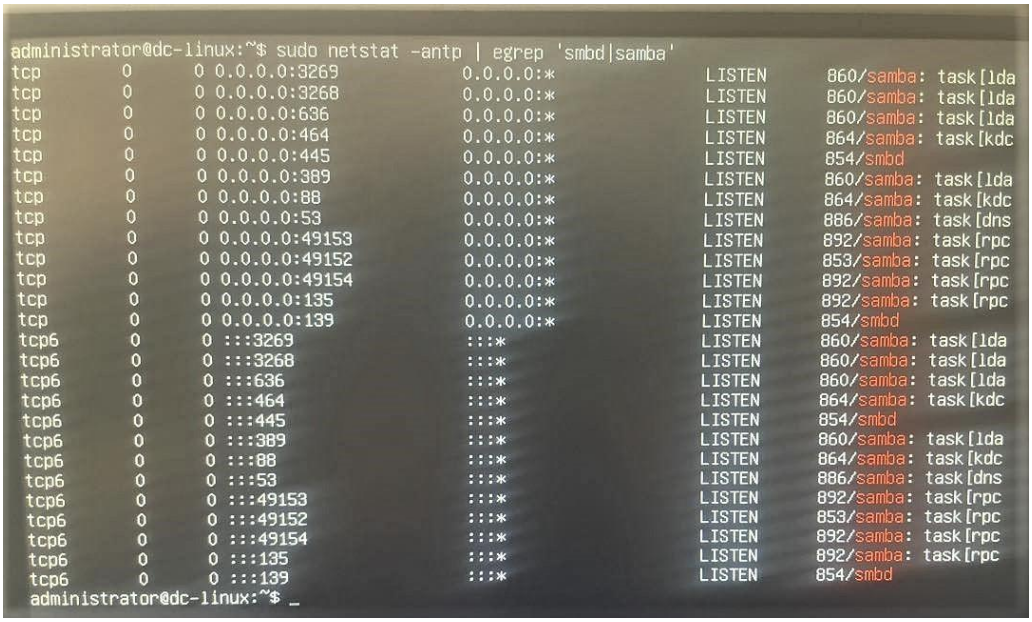
Obrázok 207 : Odmaskovanie SBS (vlastný zdroj)

Teraz je potrebné Samba ADDC povoliť.

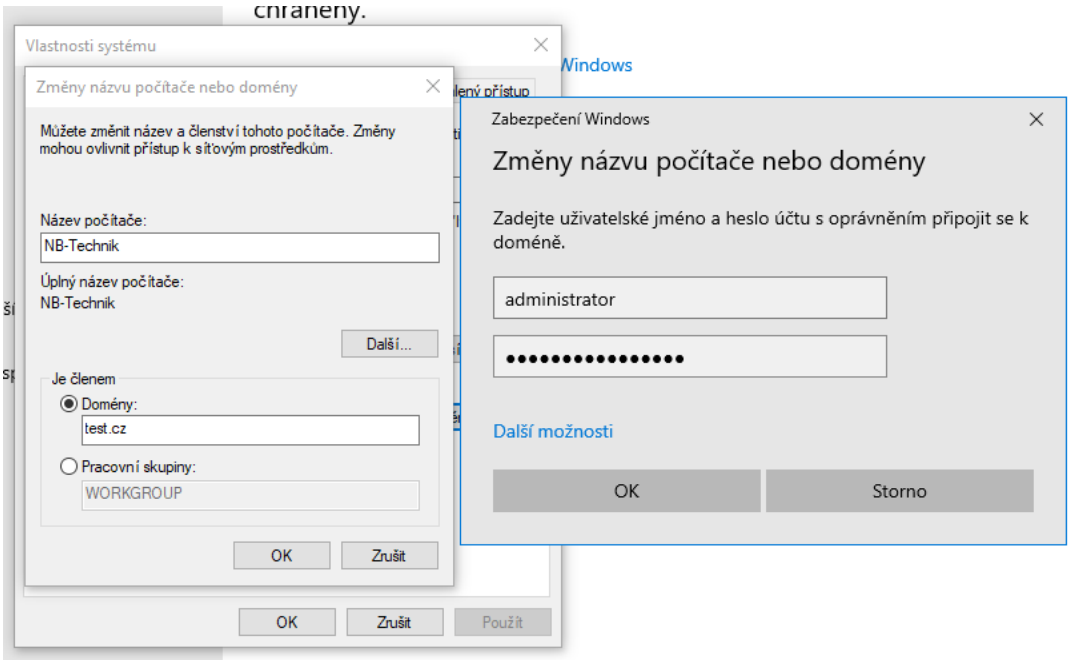


Obrázok 208 : Povolenie Samba ADDC (vlastný zdroj)

Posledným krokom je skontrolovanie portov, aby sa zistilo, či na nich Samba počúva a je aktívna.



Obrázok 209 : Prehľad portov (vlastný zdroj)



Obrázok 210 : Pripojenie testovacieho zariadenia do domény (vlastný zdroj)

Po tomto kroku je funkčná rola AD DS (teda dá sa pripojiť do domény, vytvárať užívateľov, skupiny, OU atď) a DNS. Zariadenie je potrebné reštartovať a presunúť sa ku konfigurácii ďalších rolí.

Linux a Windows sú rozdielne operačné systémy, kde právomoci a pravidlá platia inak – pokiaľ sa k nakonfigurovanému Linux radiču (ktorý využíva Sambu) pripojí klient s OS Windows, budú na neho platiť nakonfigurované Windows skupiny a politiky. Pripojenie Linux klienta do Windows domény samozrejme možné je, ale Linux bude ignorovať právomoci a pravidlá definované systémom Windows – pokiaľ by bolo teda potrebné mať hybridné prostredie, musí sa využiť software pre riadenie užívateľských účtov, skupín, rolí a oprávnení vrátane SSH kľúčov a SUDO pravidiel (napríklad FreeIPA). Konfigurácia FreeIPA je zložitosťou podobná konfigurácii doménového radiča, preto ani v práci uvedená nebude, cieľom je vysvetliť čitateľovi, že pokiaľ je potrebné hybridné prostredie (teda v infraštruktúre sú počítače s rôznymi operačnými systémami) tak musí, byť pre každý OS ošetrené riadenie užívateľských účtov, skupín, rolí a oprávnení.

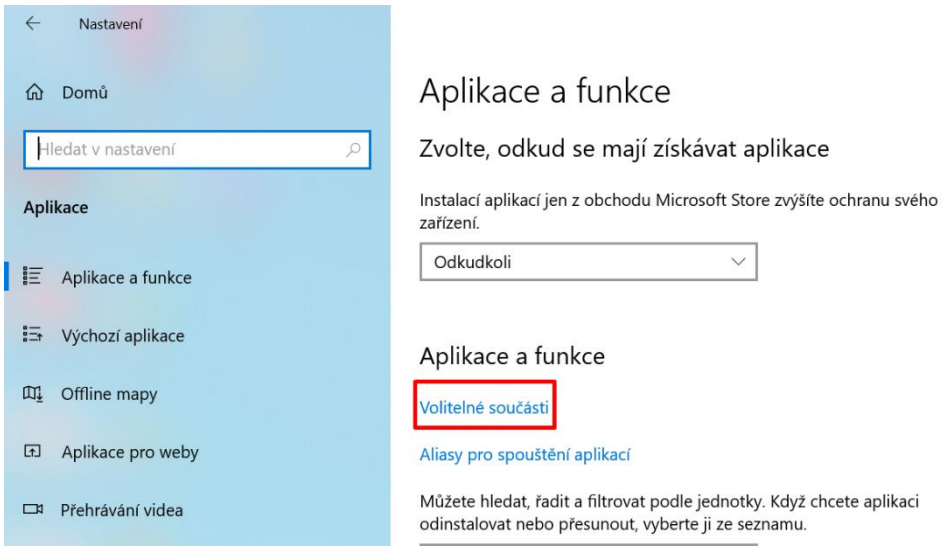
6.4 Konfigurácia ostávajúcich rolí a funkcií, nastavenie úložiska pre užívateľov

Dve role už sú nakonfigurované, ešte je potrebné nastaviť tie ostávajúce. Priamo na serveri sa role len inštalujú a nastavujú, ale spravujú sa prostredníctvom nástroja RSAT, čo je súčasťou Windowsu.

6.4.1 Nástroj RSAT

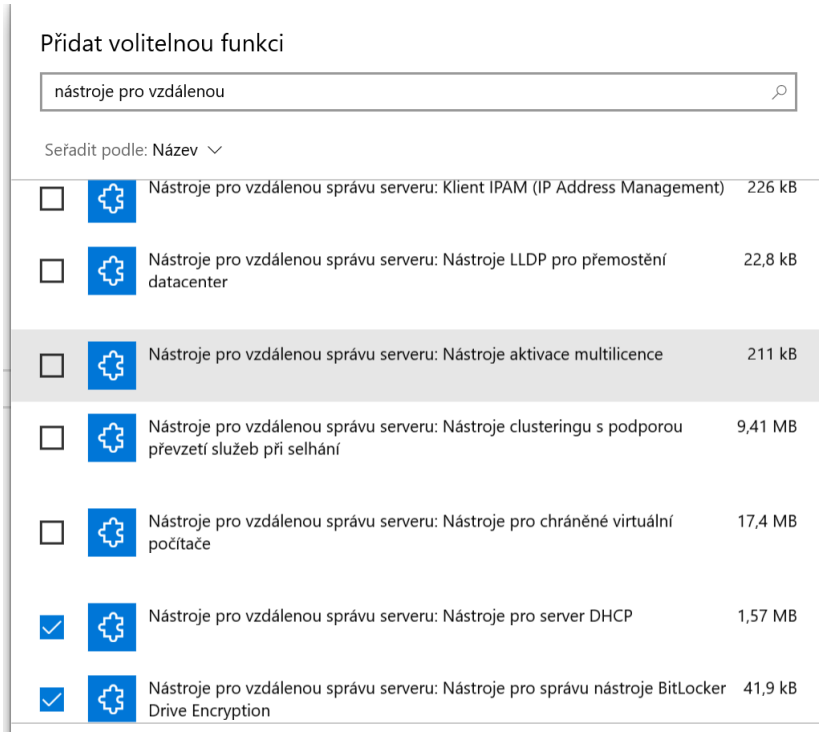
V tejto chvíli je možné počítač pripojiť do domény a následne sa prihlásiť pod administrátorským účtom. Postup pripojenia do domény je úplne rovnaký, ako pre systém Windows, pretože sa stále jedná o Windows klienta, tento krok teda dokumentovaný nebude.

Nástroj RSAT slúži pre vzdialenú správu rolí a funkcií servera z iného počítača (ale logicky zariadenie musí mať nainštalovaný operačný systém rovnakej platformy). V súčasnej dobe je tento nástroj už integrovaný, teda nie je potrebné ho sťahovať, ale je potrebná inštalácia potrebných súčastí.



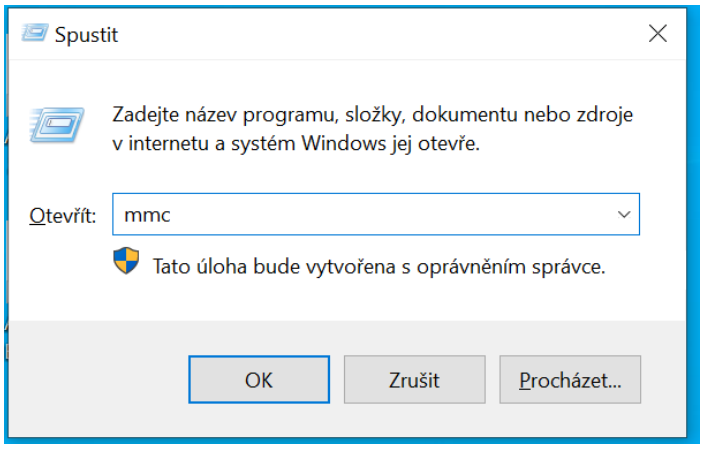
Obrázok 211 : Pridanie voliteľných súčastí (vlastný zdroj)

Následne je potrebné jednotlivé nástroje nainštalovať podľa potreby.

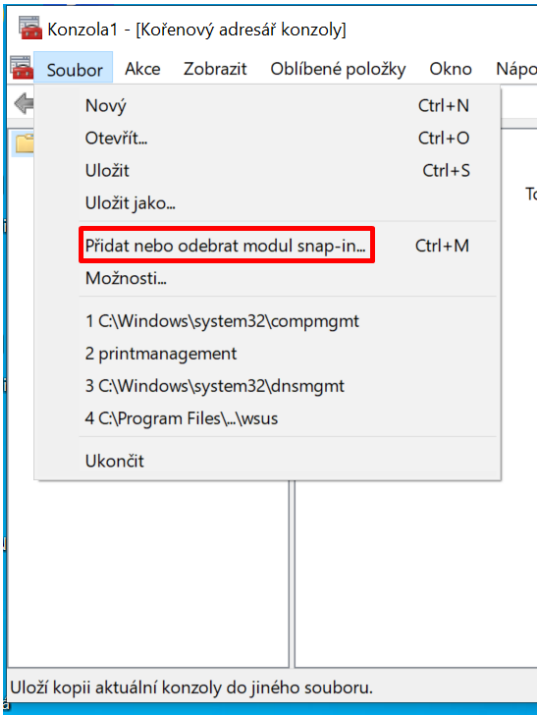


Obrázok 212 : Inštalácia voliteľných funkcií (vlastný zdroj)

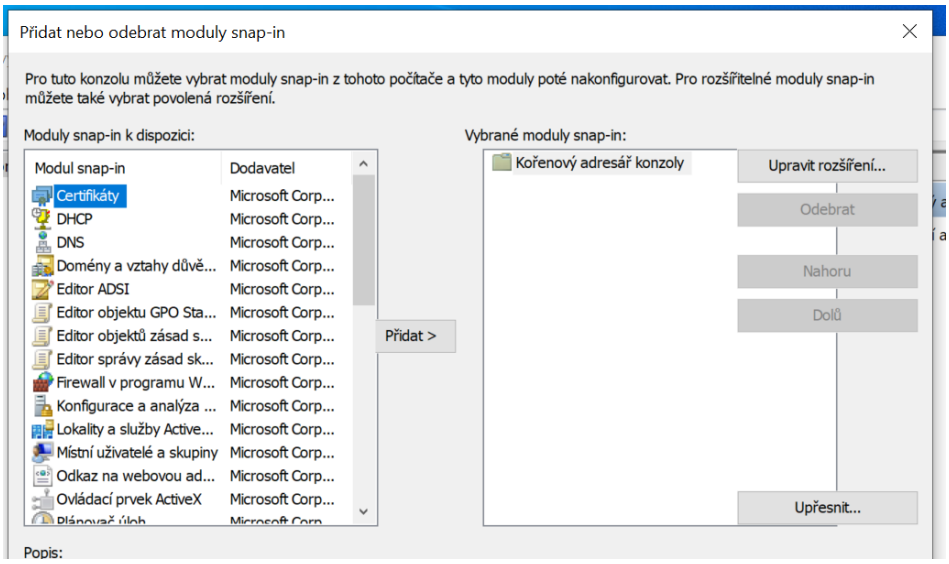
Nástroj RSAT sa dá využívať dvomi spôsobmi – pomocou nástrojov pre správu v ovládacích paneloch, alebo pomocou MMC (microsoft management console).



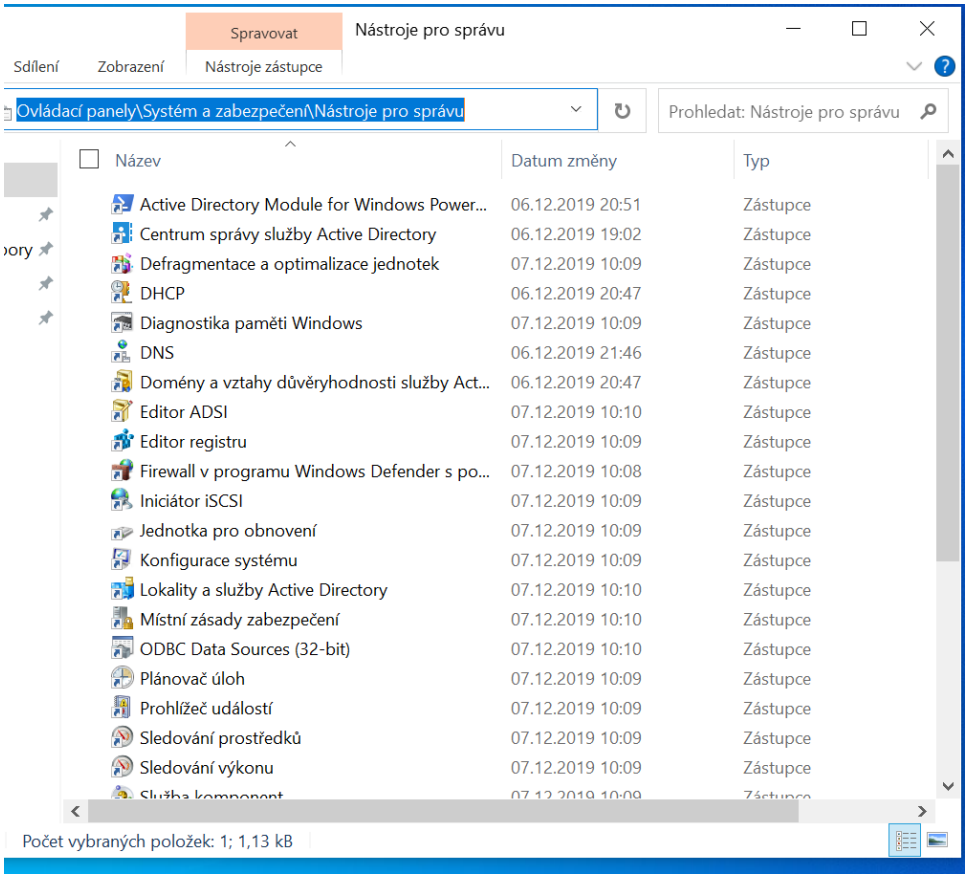
Obrázok 213 : Využitie RSAT prostredníctvom MMC (vlastný zdroj)



Obrázek 214 : Pridanie modulov (vlastný zdroj)



Obrázek 215 : Výber modulov (vlastný zdroj)

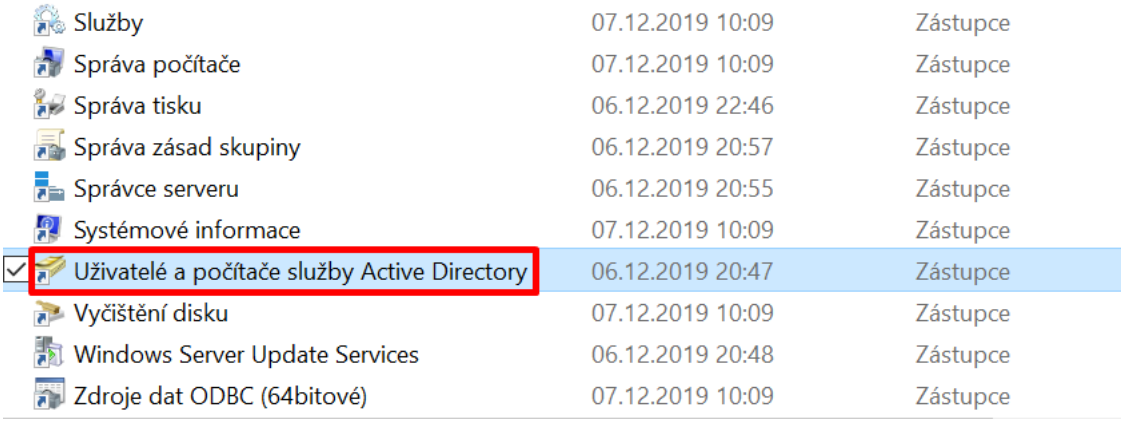


Obrázok 216 : Prístup pomocou ovládacieho panelu (vlastný zdroj)

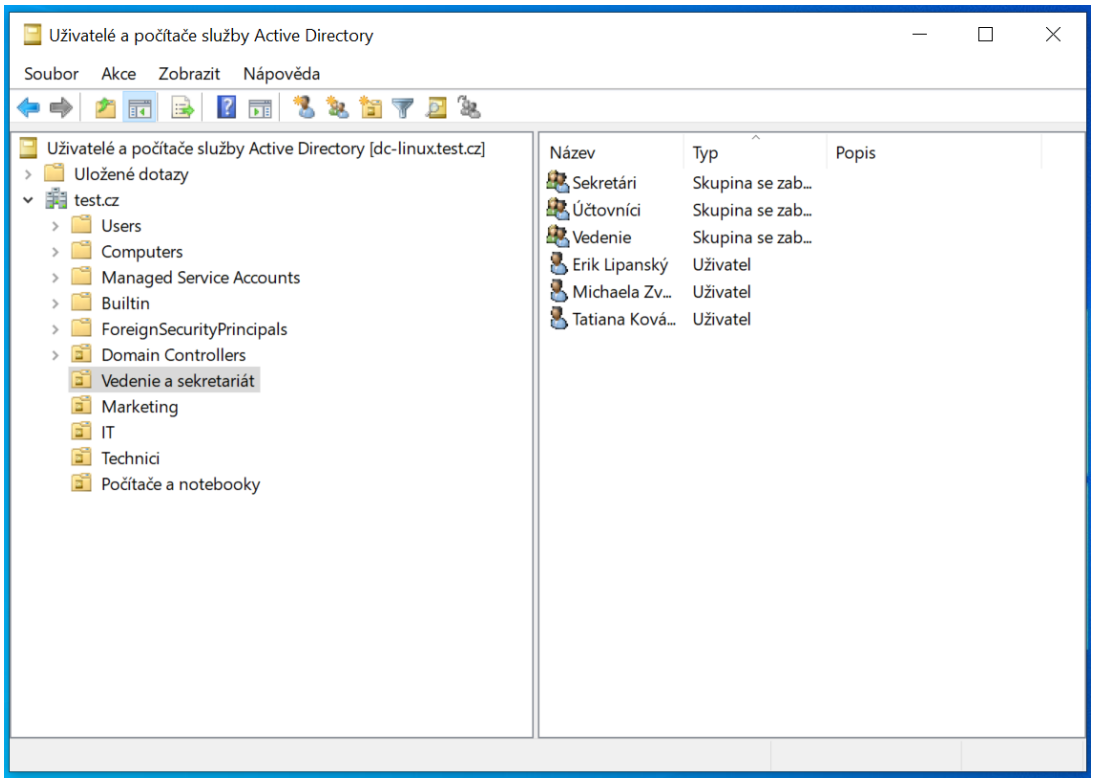
6.4.2 Konfigurácia role AD DS

Rola AD DS bola v predchádzajúcich krokoch nakonfigurovaná, teraz je potrebné ju nastaviť tak, ako to bolo v prípade Windowsu – čiže naplniť ju užívateľmi, OU, skupinami atď.

Postup plnenia je úplne rovnaký vďaka nástroju RSAT.



Obrázok 217 : Výber modulu pre AD DS (vlastný zdroj)

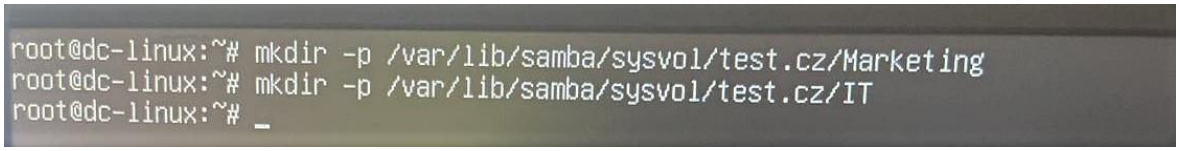


Obrázok 218 : Štruktúra AD DS (vlastný zdroj)

6.4.3 Konfigurácia úložiska pre užívateľov

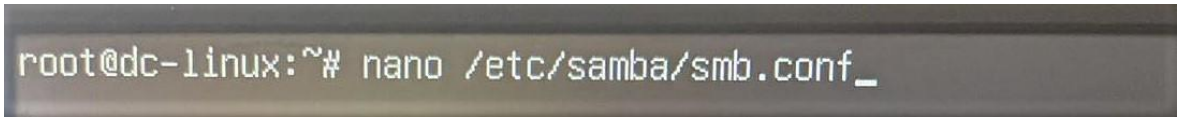
Táto podkapitola sa bude zaoberať vytvorením zdieľaných zložiek pre užívateľov. Vytvorené budú dve zdieľané zložky, a to „Marketing“ a „IT“. Nastavenia oprávnenia prístupu bude nastavené v inej kapitole.

Najprv je potrebné vytvoriť zložky, ktoré sú určené k zdieľaniu.

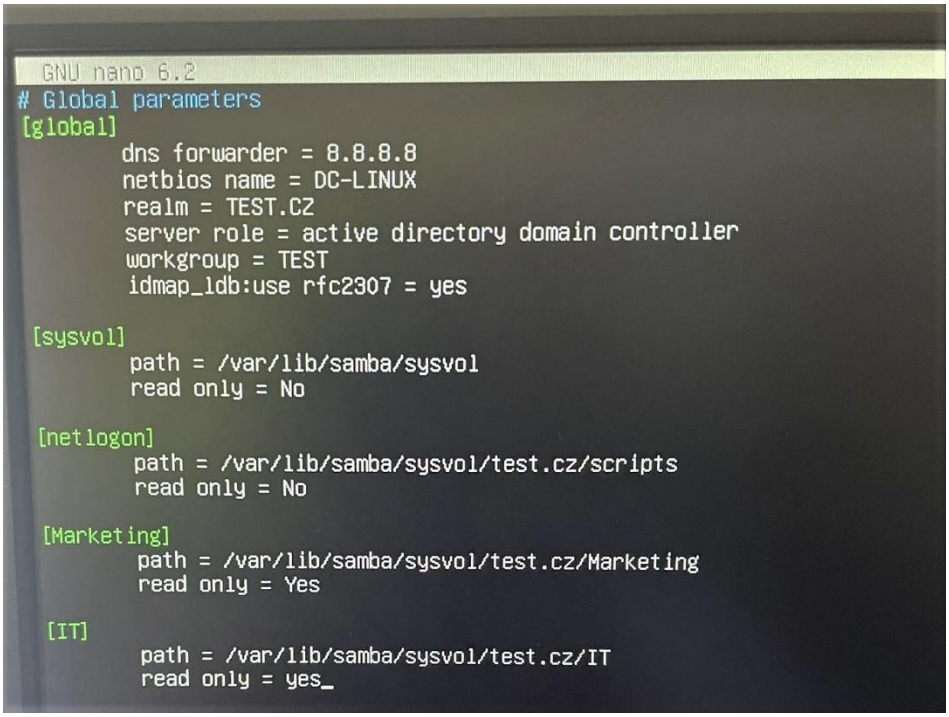


Obrázok 219 : Vytvorenie zložiek (vlastný zdroj)

Po tomto kroku nasleduje úprava smb.conf, kde je potrebné definovať cestu k daným zložkám a základné oprávnenie.

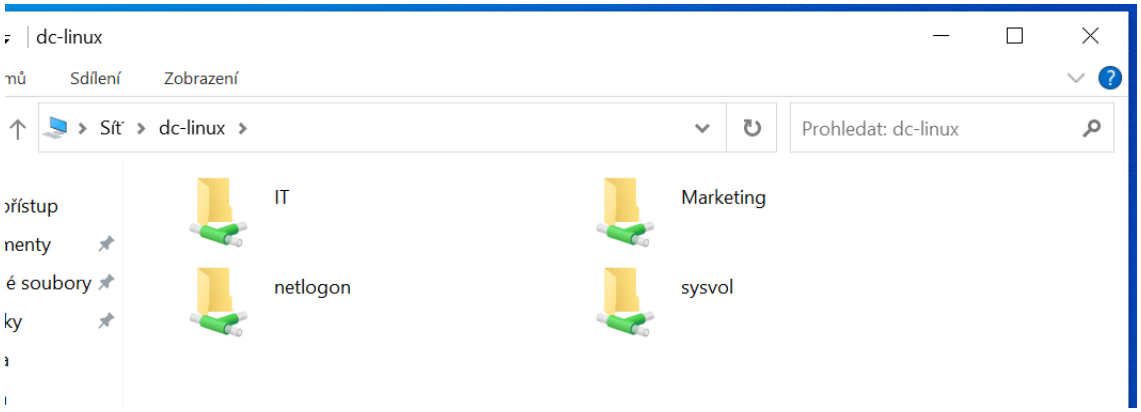


Obrázok 220 : Cesta k súboru nastavenia zdieľania zložiek (vlastný zdroj)



Obrázok 221 : Úprava súboru smb.conf (vlastný zdroj)

Ešte je potrebné otestovať, či sú zložky zdieľané a viditeľné.



Obrázok 222 : Test viditeľnosti zložiek (vlastný zdroj)

6.4.4 Konfigurácia role DHCP

Prvým krokom je inštalácia samotného DHCP serveru.

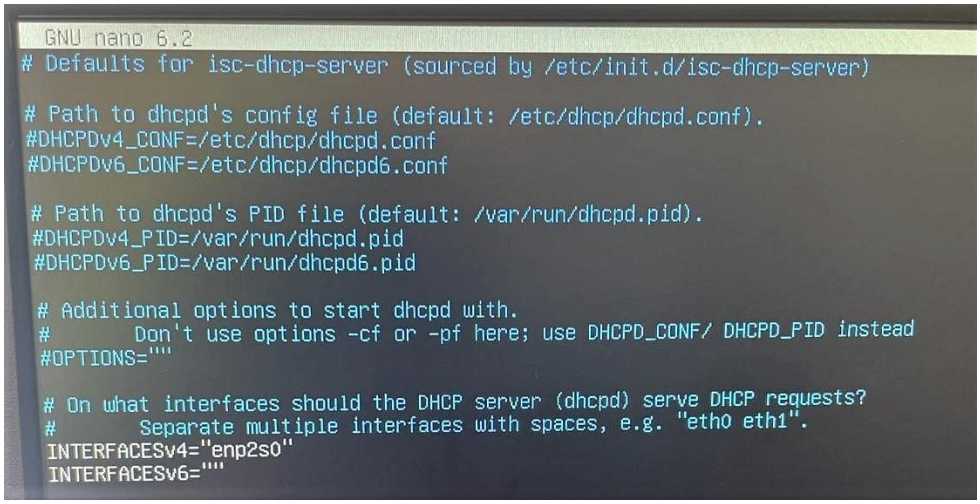
```
root@dc-linux:~# apt install -y isc-dhcp-server
```

Obrázok 223 : Inštalácia DHCP servera (vlastný zdroj)

Druhým krokom je definovanie rozhrania, na ktoré budú prichádzať žiadosti o pridelenie IP adresy. Všetky rozhranie je možné si zobraziť prostredníctvom príkazu „ip a“.

```
root@dc-linux:~# nano /etc/default/isc-dhcp-server
```

Obrázok 224 : Cesta k súboru nastavenia rozhrania (vlastný zdroj)

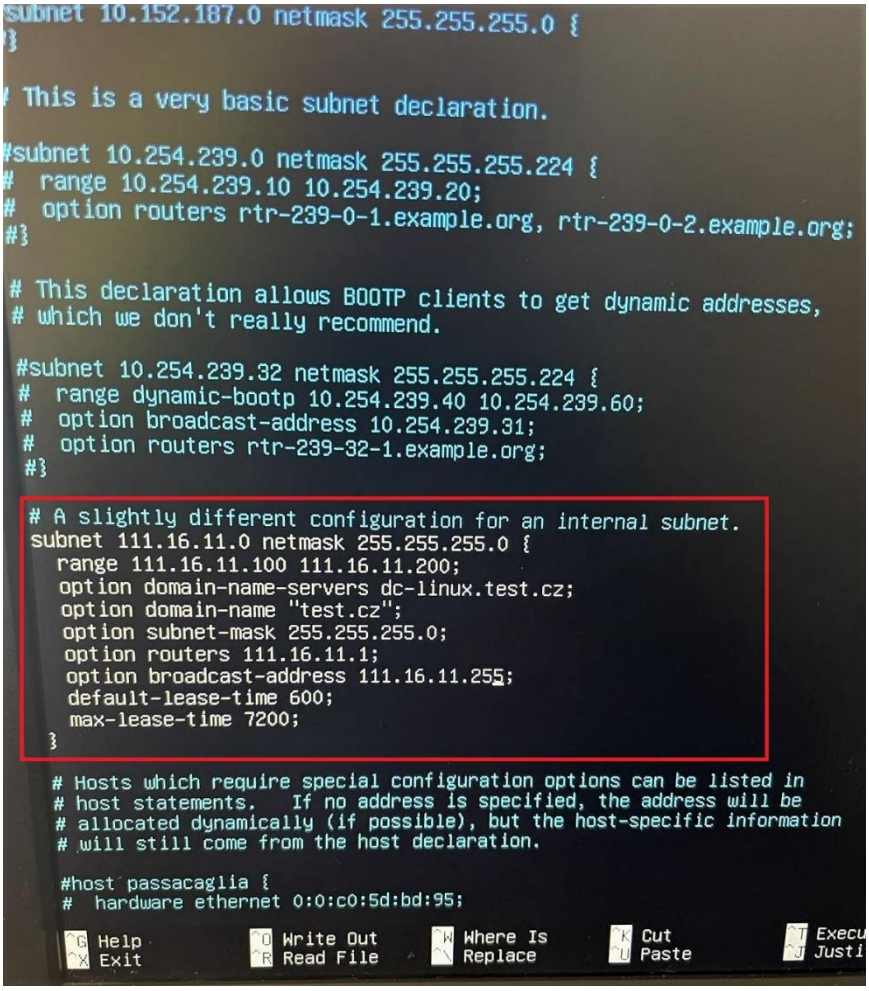


Obrázok 225 : Definovanie rozhrania pre IPv4 (vlastný zdroj)

Nasleduje samotná konfigurácia DHCP servera v súbore dhcpd.conf. Súbor môže byť prípadne zálohovaný, ako to bolo v prípade Samby, tento krok bude preskočený.

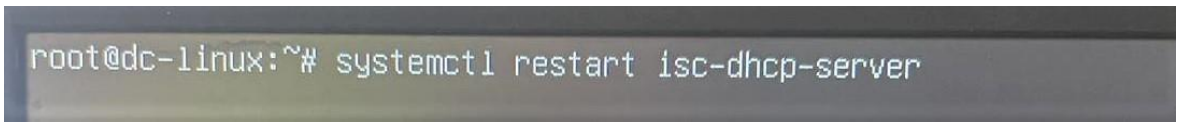
Obrázok 226 : Cesta k súboru konfigurácie DHCP (vlastný zdroj)

Po otvorení konfiguračného súboru sa nastavia rovnaké parametre, ako to bolo u systému Windows.



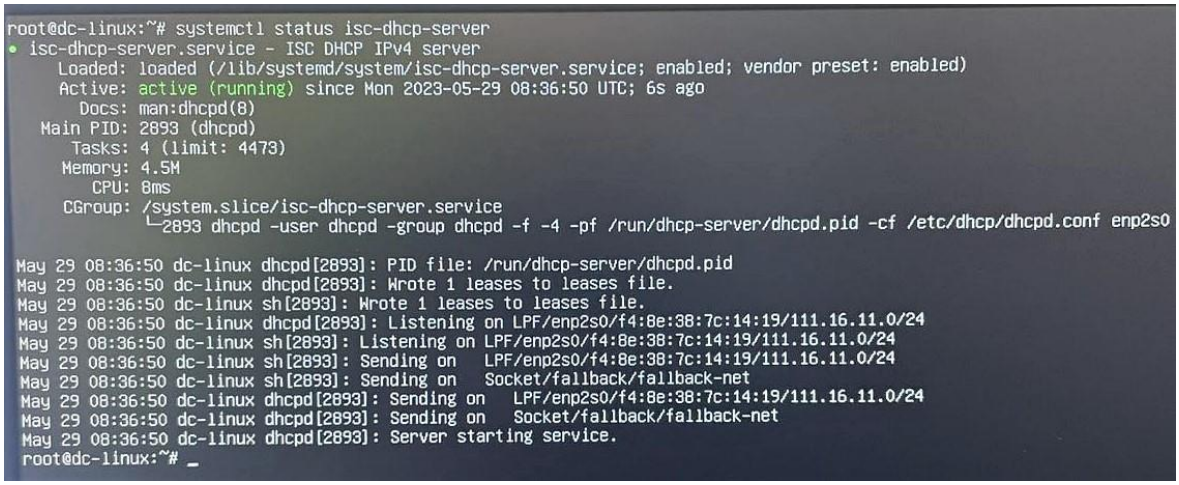
Obrázok 227 : Nastavenie potrebných parametrov DHCP (vlastný zdroj)

Službu je potrebné následne reštartovať.



Obrázok 228 : Reštart služby DHCP (vlastný zdroj)

Po reštarte nasleduje overenie funkčnosti (teda toho, či služba beží).

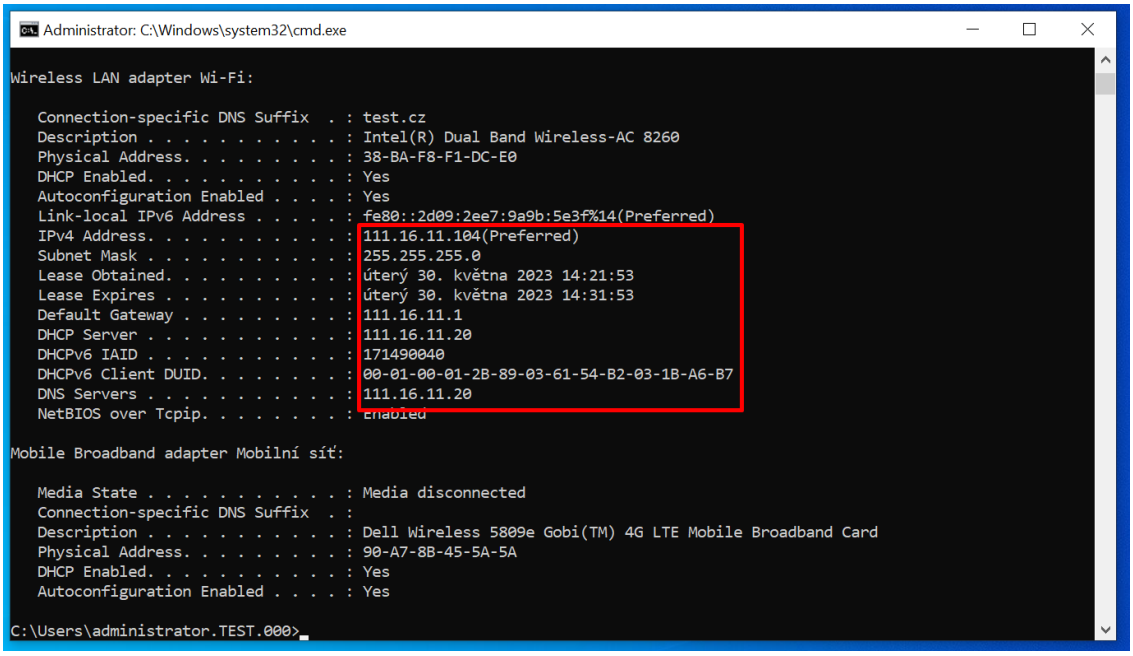


Obrázok 229 : Status služby DHCP (vlastný zdroj)

Posledným krokom je povolenie portu 67 vo firewalle (je to port pre službu DHCP).

Obrázok 230 : Povolenie portu 67 vo firewalle (vlastný zdroj)

Nastavenie DHCP sa dá jednoducho otestovať tak, že sa stačí prihlásiť na zariadenie pripojené k doméne a pozrieť si na ňom sieťovú konfiguráciu. Po konfigurácii role DHCP je potrebné vypnúť DHCP na routri a umožniť zariadeniu načítanie nových adries. DHCP funguje v poriadku, adresy sa pridelili úspešne.

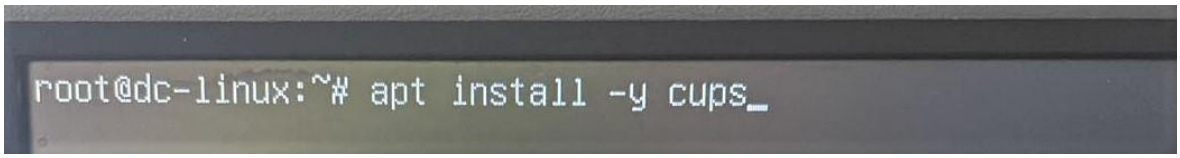


Obrázok 231 : Test DHCP

6.4.5 Konfigurácia role Print and Document Services

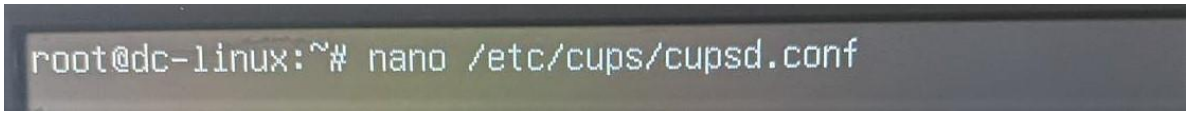
Táto rola musí byť takisto konfigurovaná na systéme Linux, kde sa nachádza pod názvom CUPS (modulárny tlačový systém).

Na začiatok je potrebné CUPS nainštalovať.

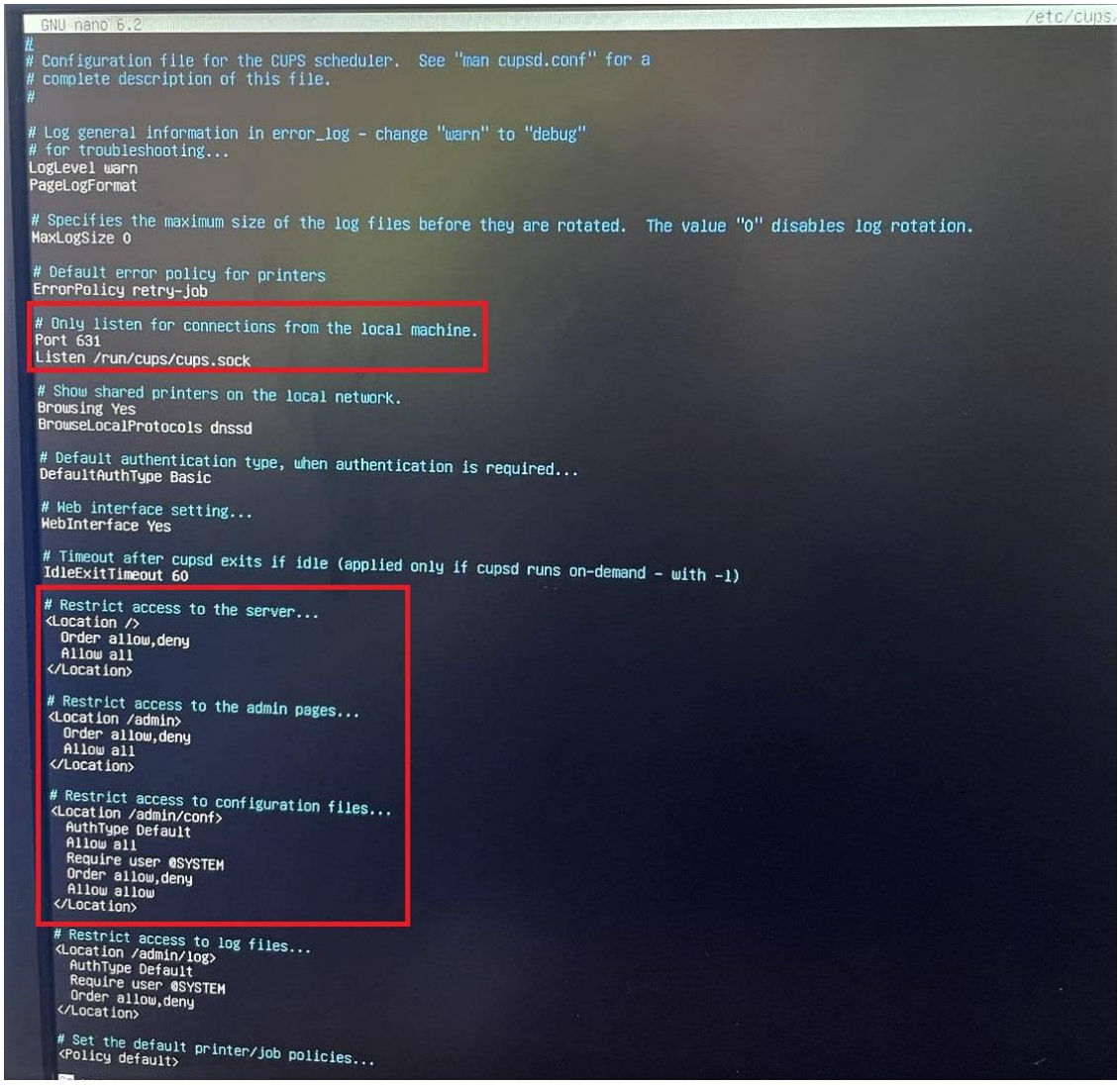


Obrázok 232 : Inštalácia CUPS (vlastný zdroj)

Ďalším krokom je konfigurácia súboru cupsd.conf tak, aby sa k CUPS dalo pristúpiť prostredníctvom webového prehliadača.

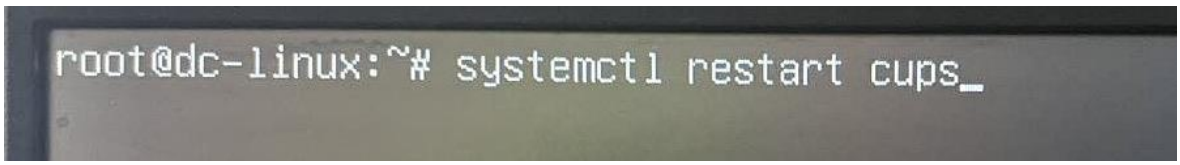


Obrázok 233 : Cesta k súboru nastavenia CUPS (vlastný zdroj)



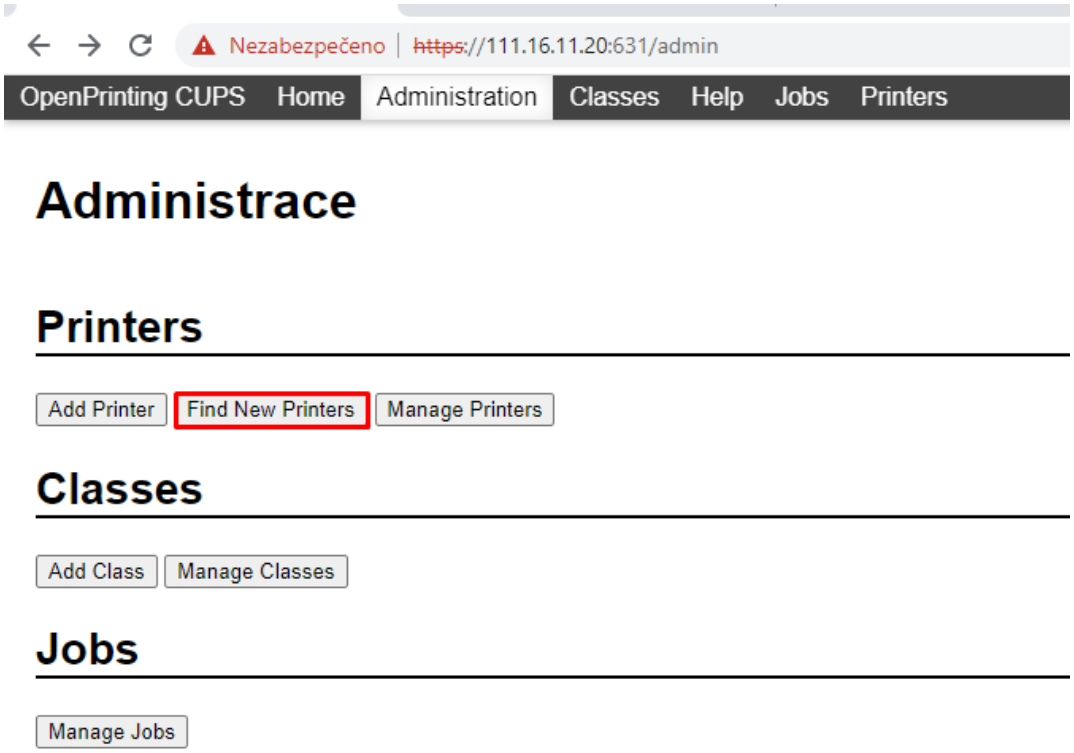
Obrázok 234 : Konfigurácia cupsd.conf súboru (vlastný zdroj)

Následne je potrebné CUPS reštartovať.



Obrázok 235 : Reštart CUPS (vlastný zdroj)

Po zadaní IP adresy 111.16.11.20:631/admin sa načítalo webové rozhranie OpenPrinting CUPS. Teraz je potrebné tlačiareň pridať, vybraná bude možnosť ich detekcie v sieti.

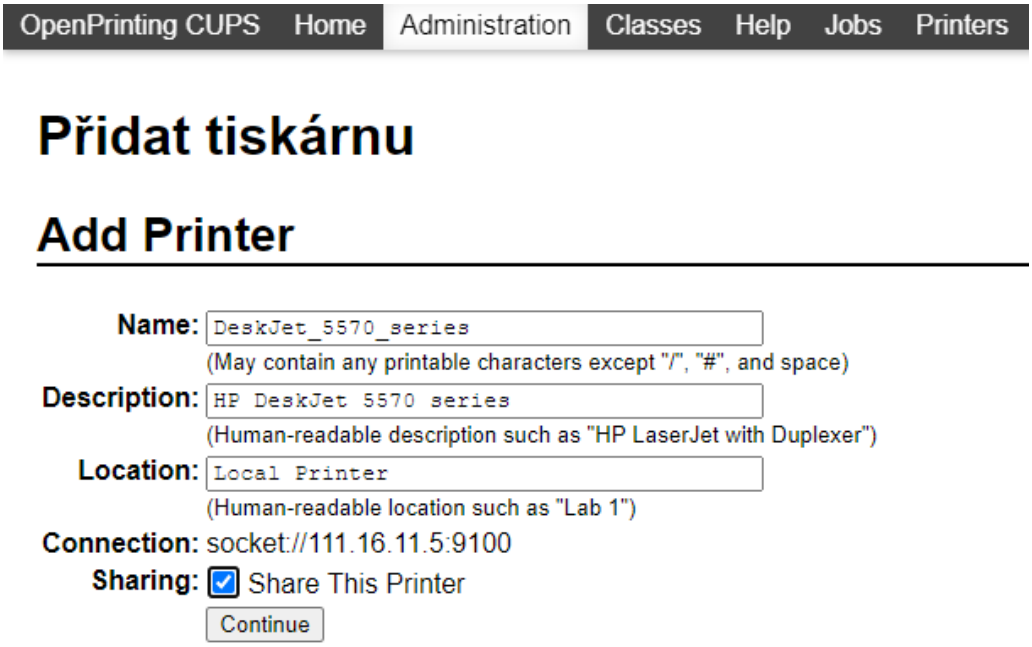


Obrázok 236 : Vyhľadanie tlačiarní (vlastný zdroj)

Následne je potrebné vybrať správnu tlačiareň zo zoznamu, výhodou je to, že sa nie je potrebné starať o ovládač pre tlačiareň.

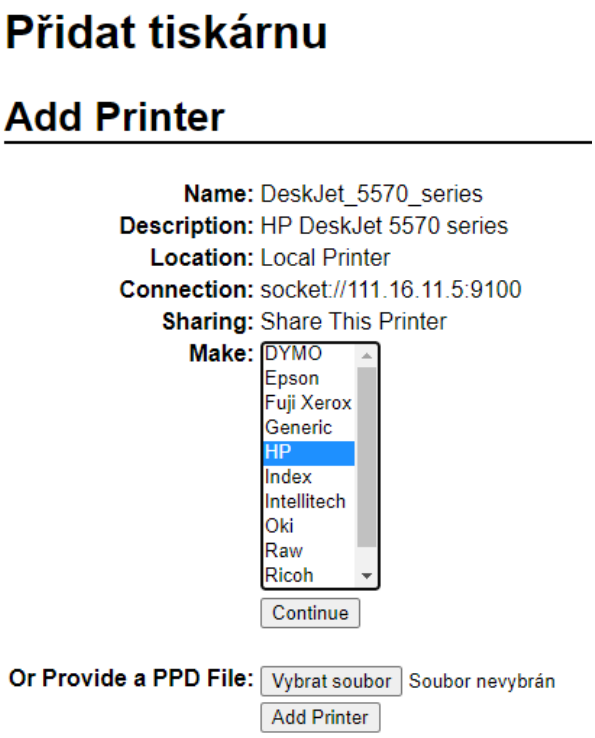
Obrázok 237 : Výber tlačiarne zo zoznamu (vlastný zdroj)

Tlačiareň potrebuje nastaviť základné parametre, akými je názov, popis a umiestnenie. Okrem toho je ešte potrebné zaškrtnúť políčko „Sharing“.



Obrázok 238 : Definovanie názvu, popisu, umiestnenia a zdieľania pre tlačiareň (vlastný zdroj)

Následne je potrebné vybrať výrobcu tlačiarne – to zabezpečí výber správneho ovládača.

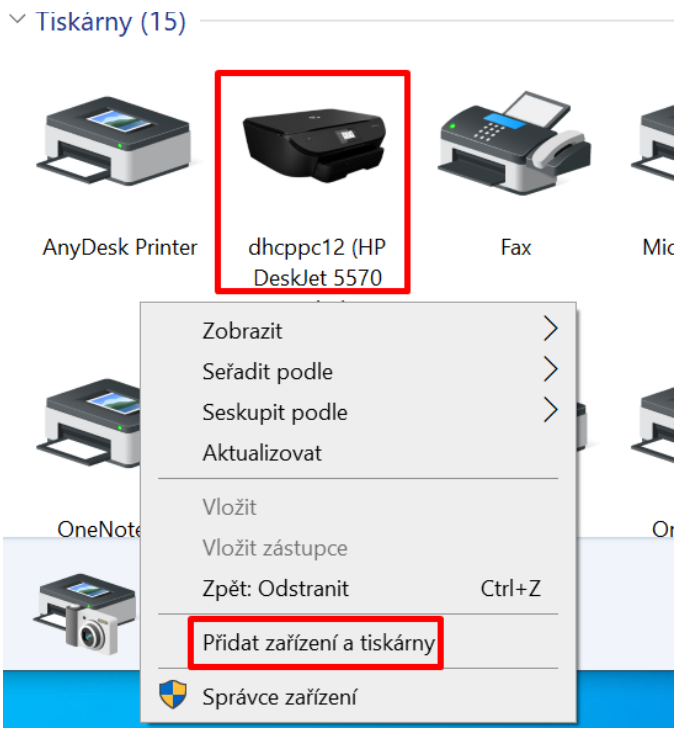


Obrázok 239 : Výber výrobcu tlačiarne (vlastný zdroj)

Následne je potrebné tlačiarni nastaviť vlastnosti tlače.

Obrázok 240 : Nastavenie vlastností tlače (vlastný zdroj)

Po tomto kroku je tlačiareň úspešne nakonfigurovaná a funkčná, ale je ju ešte potrebné pridať počítaču pomocou ovládacieho panelu. Na obrázku nižšie je vidieť už hotová pridaná tlačiareň.



Obrázok 241 : Pridanie tlačiarne zariadeniu (vlastný zdroj)

6.4.6 Konfigurácia role WSUS

Role WSUS ako bolo spomenuté už predtým slúži na automatické aktualizácie serverov, počítačov a notebookov v sieti. WSUS je bohužiaľ rola, ktorá nie je konfigurovateľná na Linux serveroch (čo je aj celkom pochopiteľné, keďže sa jedná o úplne iný operačný systém). To ale neznamená, že nie je možné disponovať Linux doménovým radičom a mať automatické aktualizácie Windows klientov a serverov. Problém je ale v tom, že by do infraštruktúry musel pribudnúť iný Windows server, ktorý by túto rolu plnil – pripojiť ho do domény by takisto nebolo problémom. Základným problémom je, že by bolo potrebné zakúpiť licenciu na Windows server bez ohľadu na to, či by na serveri bežala len jedna služba. Okrem licencie na samotný Windows server by boli ešte potrebné špeciálne CAL licencie, aby mohol WSUS fungovať.

V predošlej kapitole praktickej časti je využité zariadenie, ktoré má nakonfigurovaný WSUS, ale samo o sebe je doménovým radičom s rovnakou konfiguráciou, ako má tento doménový radič na systéme Linux – teda je nereálne jeho využitie na tento účel, musel by prejsť úpravou.

6.4.7 Konfigurácia funkcie BitLocker

BitLocker podobne ako rola WSUS nie je na tom najlepšie, avšak tu sa jedná o kozmetické, nie funkčné vady. BitLocker je spustiteľný na ktoromkoľvek Windows zariadení – ale pokiaľ je konfigurovaný na radiči, tak sa viaže na GPO, kde má nakonfigurované politiky (napríklad typ šifrovania, dĺžka kľúča atď.) a zároveň ukladá kľúč na samotný radič. V tomto prípade sa teda nedá funkcia BitLocker konfigurovať na radiči, tak má nastavené preddefinované parametre (ktoré sú na druhej strane odporúčané, takže sa to nedá považovať za veľké obmedzenie). Pokiaľ je na zariadení spustené šifrovanie prostredníctvom BitLocker, kľúč sa musí v každom prípade exportovať (najčastejšie do textového súboru) a tým sa dá v podstate administrátorom preniesť na flash disku a dané kľúče aspoň ručne ukladať na Linux doménovom radiči, aby nedošlo k ich strate.

Linux zariadenia môžu namiesto BitLockeru využiť VeraCrypt, alebo TrueCrypt.

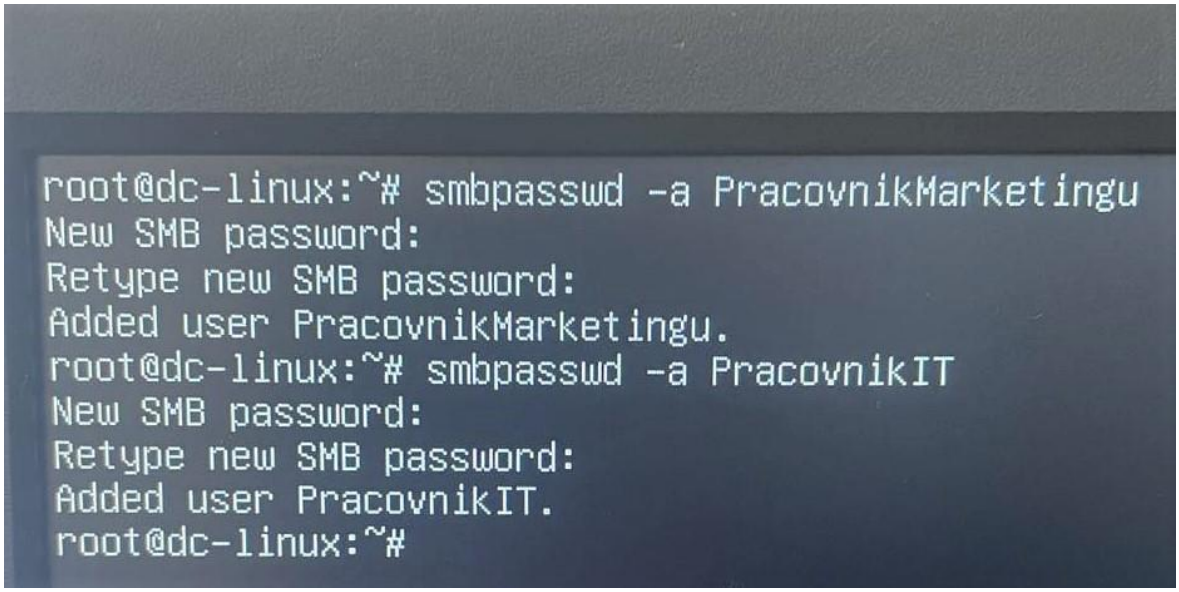
6.5 Zabezpečenie doménového radiča a jeho zdrojov

Zabezpečenie Linux doménového radiča je veľmi podobné, ako je to u systému Windows, nakoniec sa stále jedná o server v roli doménového radiča, pre ktorú sú definované bezpečnostné kroky a dajú sa dohľadať na internete. V jednej veci má však operačný systém Linux navrch – nie je tak často využívaný, ako systém Windows, s čím súvisí menšie množstvo vyvíjaného škodlivého software a útokov. To však nie je jediný dôvod, pre ktorý je operačný systém Linux bezpečnejší, dôvody sú komplexne popísané v citovaném článku. [29]

6.5.1 Nastavenie prístupu k zdrojom

Nastavenie prístupu k zdrojom (teda k testovacím zložkám „IT“ a „Marketing“) nemôže byť nastavený rovnakým spôsobom, ako to bolo u systému Windows, pretože Linux DC by neakceptoval nastavenie bezpečnostných skupín. Namiesto toho sa dá prístup nastaviť veľmi podobným spôsobom, ale s využitím užívateľov pre Sambu.

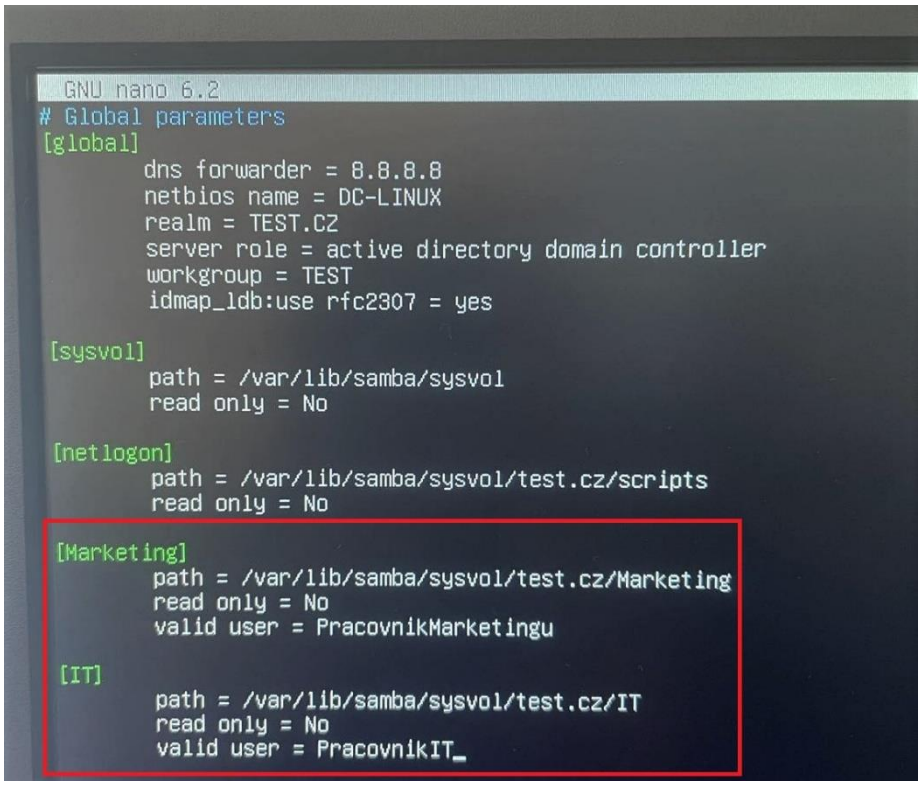
Prvým krokom teda je vytvoriť a nastaviť užívateľov, ktorí majú mať k zdieľaným zložkám prístup. Vytvoria sa teda užívatelia „PracovnikMarketingu“ a „PracovnikIT“.



Obrázok 242 : Vytvorenie užívateľov (vlastný zdroj)

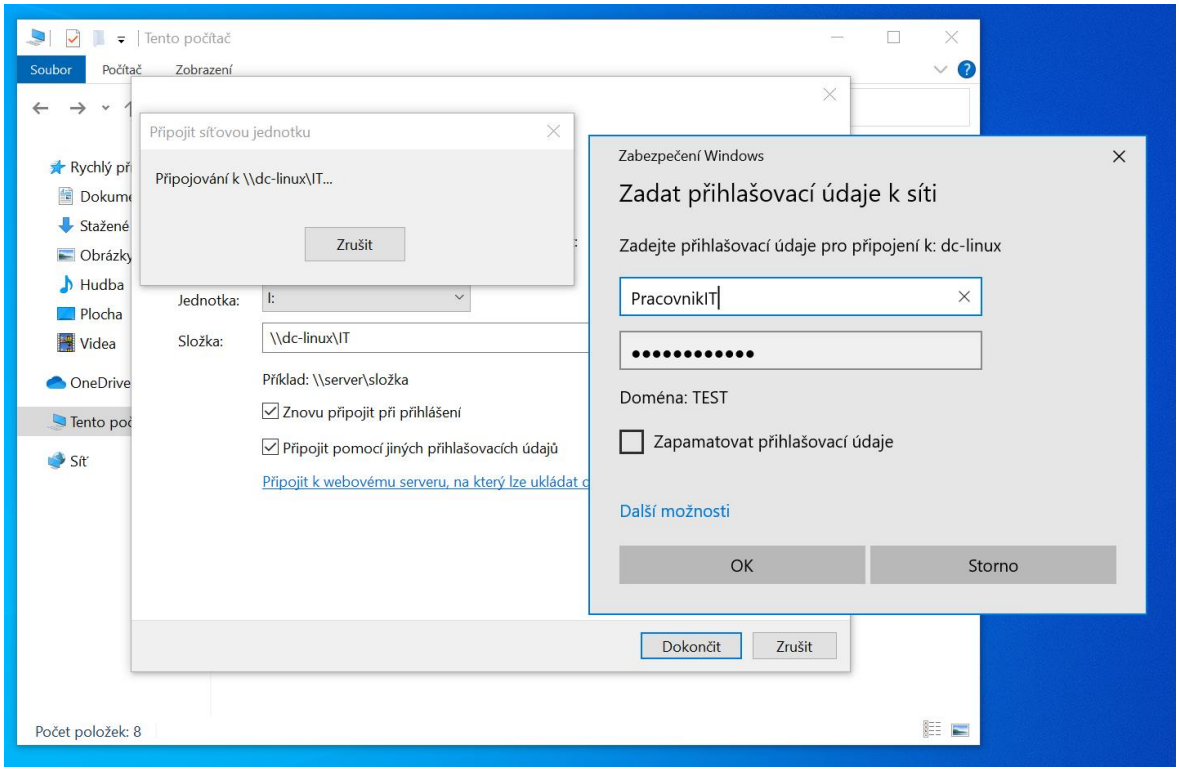
Teraz je potrebné nakonfigurovať súbor smb.conf. Konkrétne je potrebné definovať užívateľov, ktorí k daným zložkám môžu pristupovať.

Obrázok 243 : Cesta k súboru nastavenia smb.conf (vlastný zdroj)

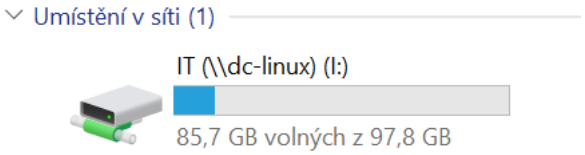


Obrázok 244 : Konfigurácia prístupu k zložkám (vlastný zdroj)

Po tomto kroku sú zložky kompletne nastavené pre prístup príslušných užívateľov. Ostáva skúsiť pristúpiť k zložke z testovacieho zariadenia. Mapovanie zložky je rovnaké, ako v prípade systému Windows, avšak je potrebné zadať meno a heslo užívateľa, ktorý má oprávnenie do zložky vstúpiť.



Obrázok 245 : Mapovanie zdieľanej zložky (vlastný zdroj)



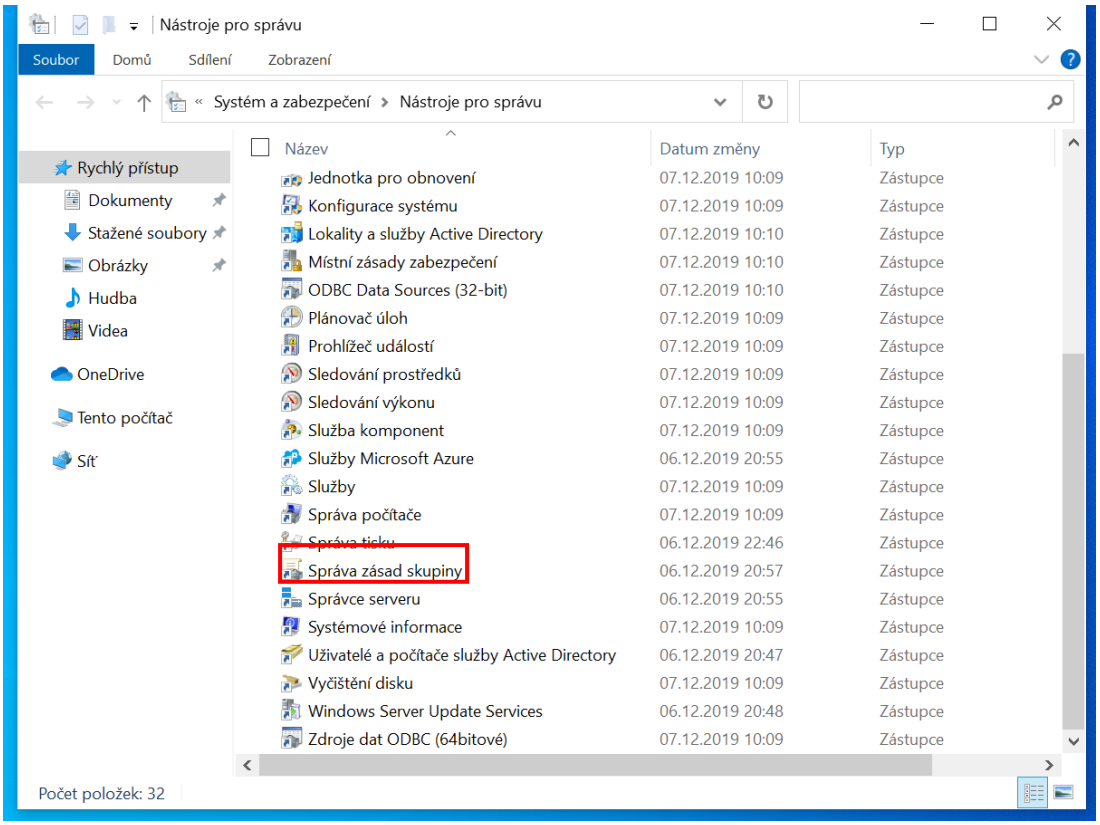
Obrázok 246 : Umiestnenie v sieti (vlastný zdroj)

6.5.2 Konfigurácia skupinových politík

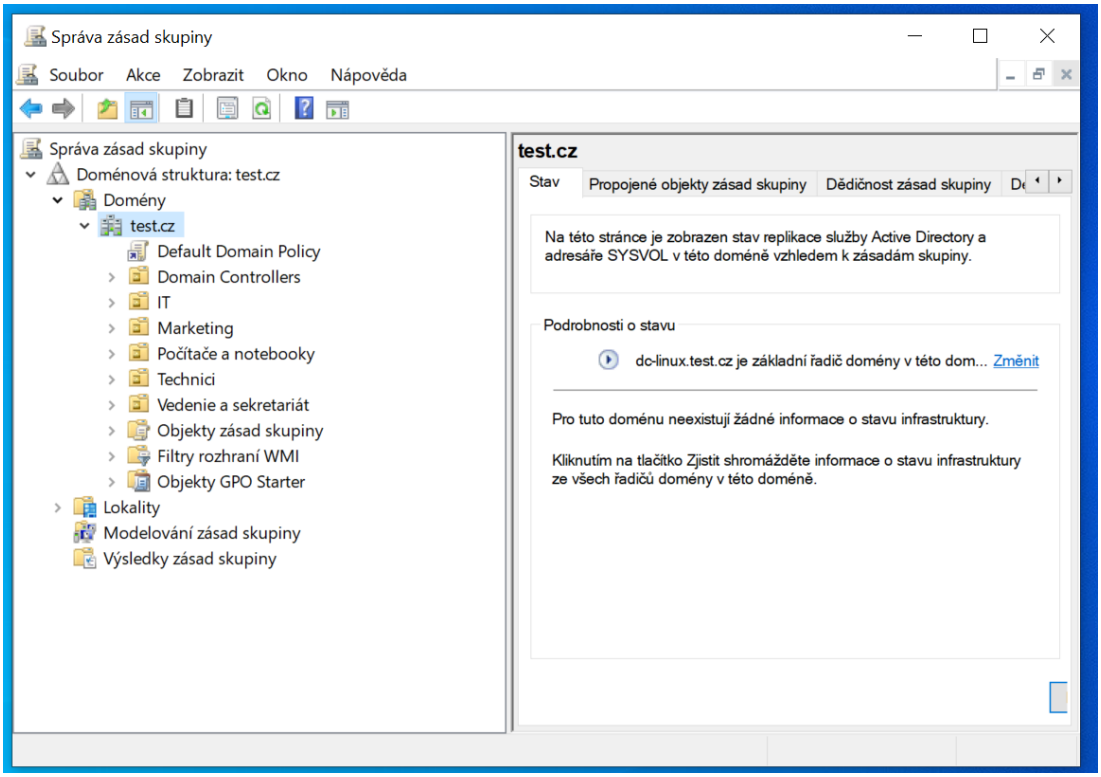
Skupinové politiky sa dajú jednoducho konfigurovať prostredníctvom nástroja RSAT. V prípade Linux klienta Windows GPO nefungujú, takže je potrebné využiť software FreeIPA, ktorý politikami disponuje.

Pri konfigurácii pomocou nástroja RSAT je vždy potrebné definovať DC, ktorého role a funkcie sa majú konfigurovať / spravovať. Keďže je zariadenie pripojené v doméne, tak si dokáže dané DC vyhľadať automaticky.

Politiky sa konfigurujú úplne rovnako, ako na Windows doménovom radiči, preto samotná konfigurácia a testovania nebudú uvedené, keďže už sú raz dokumentované u systému Windows. Z hľadiska funkcionality funguje úplne rovnako, takže testovacia časť vyšla takisto kladne.



Obrázok 247 : Výber nástroja „Správa zásad skupiny“ (vlastný zdroj)



Obrázok 248 : Konfigurácia funkcie „Správa zásad skupiny“ (vlastný zdroj)

Týmto je teda konfigurácia Linux doménového radiča u konca.

Jedným z bodov zadania je porovnanie obidvoch variant – tento bod nájde čitateľ v závere, kde sa štylisticky hodí viac, než samostatná kapitola práce.

ZÁVER

Konfigurácia doménových radičov je beh na dlhú trať – od návrhu, čo musí doménový radič spĺňať, cez konfiguráciu až po zvyšovanie jeho efektivity do budúcnosti (teda je potrebné rozmýšľať veľa krokov dopredu – aký hardware zvoliť, akú verziu operačného systému zvoliť, akým spôsobom vytvoriť jeho štruktúru, aby dávala logický zmysel atď. Porovnanie a hodnotenie doménových radičov konfigurovaných v praktickej časti DP sa veľmi odvíja od osobného pohľadu technika, ktorý ich konfiguroval.

Konfigurácia doménového radiča na systéme Windows je z užívateľského hľadiska pomerne veľmi dobre logicky spracovaná – koniec koncov, doménové radiče na systémoch Windows sa využívajú bežne a takmer každý zamestnanec v IT sektore s ním príde do kontaktu. Čo sa však už pochváliť nedá je citlivosť systému a zložitosť konfigurácie. Všetky doménové radiče sú extrémne citlivé na zmenu IP adresy, alebo ich názov, pokiaľ sa uskutoční taká operácia, sú schopné sa kompletne rozbiť a vhodné sú už len na preinštalovanie alebo obnovu zo zálohy. Čo sa týka zložitosti konfigurácie, tá je zložitá v tom, že sa skladá z veľmi veľa krokov (čo sa prejavilo aj na rozsahu práce) a je potrebný neustály reštart zariadenia, aby sa zmeny prepisovali. Je nutné mať v pamäti, že doménový radič je kritickým prvkom v štruktúre, preto by sa mal napríklad nachádzať za firewallom. Na bezpečnosti nepridáva ani user – friendly prostredie, v ktorom sa veľmi rýchlo dokáže zorientovať aj človek, ktorý má minimum skúseností – avšak toto je aj výhoda, čo sa týka vzdelávacích účelov. Ďalším odradzujúcim faktom je cena licencie za Windows Server edície, tá sa odvíja od počtu jadier, pričom minimum je 16 jadier. Teda napríklad za licenciu pre Windows Server Standard 2022 pre 16 jadier je potrebné zaplatiť sumu cca 30 000 CZK (licencia je trvalá) – a to sa ešte jedná o OEM licenciu. Licencia musí byť zakúpená pre 16 jadier bez rozdielu na to, či dané zariadenie disponuje len napríklad ôsmimi jadrami. Licencovanie systému Windows (hlavne teda serverov) je komplikovaná záležitosť, pokiaľ chce distribútor predávať licencie, musí k tomu dostať špeciálne školenie. Mimo tejto základnej licencie na server ešte existujú aj CAL a RDS licencie, ktoré musia byť zakúpené, pokiaľ sa využívajú služby serverového software.

Konfigurácia doménového radiča na systéme Linux je skôr experimentálna záležitosť – v úvode kapitoly konfigurácie doménového radiča bolo uvedené, že sa dá postaviť plnohodnotný doménový radič na systéme Linux s využitím Samby. To pravdou je, ale len za určitých podmienok. Zo začiatku konfigurácia prebiehala veľmi hladko a bezproblémovo, bola mnohonásobne rýchlejšia, než bola konfigurácia doménového radiča na systéme

Windows. Prvé problémy sa vyskytli u role WSUS – tá byť nakonfigurovaná nemohla, pretože na ňu by bol potrebný iný Windows server vo vybudovanej sieťovej štruktúre, ktorý by túto rolu plnil. Alternatívy k WSUS síce existujú, ale podľa recenzií iných technikov skôr spôsobia viac problémov než úžitku. Alternatíva vyskúšaná bola, avšak nefungovala, preto ani nebola do práce vôbec zahrnutá.

Menší problém sa ešte vyskytol pri konfigurácii funkcie BitLocker – nejedná sa však o plnohodnotný problém, jedinou kozmetickou vadou bolo to, že sa kľúč neukladal na doménový radič ako to bolo pri systéme Windows. To sa však stále dá riešiť tým, že kľúč sa musí aj tak exportovať do textového súboru, ktorý sa následne fyzicky môže preniesť na doménový radič a tam sa uložiť. A samozrejme je nevýhoda v tom, že sa funkcia nedá konfigurovať prostredníctvom bezpečnostných politík (napríklad šifrovanie, dĺžka kľúča atď.).

Toto riešenie má obrovskú výhodu v cene – nie je potrebné zakupovať žiadne licencie a doménový radič môže byť plnohodnotne využívaný, vrátane využívania služieb serverového software (ktorý ale musí byť kompatibilný so systémom Linux). Je tu jedno veľké ale – pokiaľ sa v štruktúre vyskytne server so systémom Windows, tak už je potrebná licencia (čím by sa teda neoplatil server, na ktorom by bežal WSUS, to už by sa mohol rovno nakonfigurovať doménový radič na systéme Windows).

Teda toto riešenie je vhodné skôr pre malé firmy / testovacie účely, kde nie je potrebná tak veľká automatizácia (teda napríklad počítače sa aktualizujú ručne, kľúč BitLocker sa prenáša atp.).

Čo sa týka bezpečnosti, Linux servery sú celkovo oproti Windows serverom bezpečnejšie a to hneď z niekoľkých dôvodov. Tým prvým je, že väčšinou nevyužívajú grafické prostredie (ovládanie príkazmi je náročnejšie) a okrem toho má systém inú štruktúru. Tým druhým je, že systémy Windows sú celosvetovo veľmi rozšírené a najviac využívané – s čím priamočiaro súvisí exponovanie vyššiemu množstvu útokov a hľadania štrbín v systéme.

Na samotný záver sa nedá posúdiť, ktorý z nich je lepší, skôr ide o to, k akým účelom budú využívané. Prípadne si čitateľ môže urobiť názor po prečítaní práce sám.

ZOZNAM POUŽITEJ LITERATÚRY

[1] VOJTĚŠEK, Jiří, 2012. Internet a jeho služby. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. ISBN 978-80-7454-217-6.

[2] Private vs. Public IP Address Classes [online]. 31.08.2020 [cit. 2022-10-05]. Dostupné z: https://curryncode.com/2020/08/31/privatepublic-ess-classes/

[3] Comparison of "peer-to-peer" vs "client-server" Network Models [online]. 09.10.2022 [cit. 2022-10-09]. Dostupné z: https://www.networkstraining.com/peer-to-peer-vs-client-server-network/

[4] Difference between Internet and Extranet [online]. 09.10.2022 [cit. 2022-10-09]. Dostupné z: https://www.geeksforgeeks.org/difference-between-internet-and-extranet/

[5] BOUŠKA, Petr. Co je to SSO? [online]. 18.06.2014 [cit. 2022-10-26]. Dostupné z: https://www.samuraj-cz.com/clanek/kerberos-cast-3-single-sign-on-a-protokol-kerberos/

[6] BOUŠKA, Petr. Kerberos protokol a Single sign-on [online]. 06.03.2014 [cit. 2022-10-26]. Dostupné z: https://www.samuraj-cz.com/clanek/kerberos-protokol-a-single-sign-on/

[7] DOMANICKÝ, Tomáš. História operačných systémov [online]. 27.10.2022 [cit. 2022-10-27]. Dostupné z: https://docplayer.cz/61224533-Historia-operacnych-systemov-ing-tomas-domanicky.html

[8] PECINOVSKÝ, Josef a Rudolf PECINOVSKÝ. Windows 10: průvodce uživatele. Druhé, přepracované a aktualizované vydání. Praha: Grada Publishing, 2019. Průvodce. ISBN 9788027124381.ac

[9] ZOBEC, Michal. Co to je Secure Boot? [online]. 18. 9. 2021 [cit. 2022-11-08]. Dostupné z: https://www.michalzobec.cz/co-to-je-secure-boot-8313

[10] STANIK, Rastislav. Súborové systémy - I [online]. 15. 4. 2004 [cit. 2022-11-08]. Dostupné z: https://www.abclinuxu.cz/clanky/system/suborove-systemy-i

[11] MIRANDELA VIVEIROS, Betty Giovanna. Operačné systémy Funkcia a zloženie OS. [online]. 09.11.2022 [cit. 2022-11-09]. Dostupné z: https://slideplayer.cz/slide/14892305/

[12] OTIENO, John. What is the Difference Between UEFI and Legacy? [online]. 09.11.2021 [cit. 2022-11-09. Dostupné z: https://linuxhint.com/difference-between-uefi-and-legacy/

[13] MELIŠKO, Jan. Software a základné pojmy operačných systémov [online]. 09.01.2017 [cit. 2022-11-09]. Dostupné z: https://melisko.webnode.sk/news/software-a-zakladne-pojmy-operacnych-systemov/

[14] SHARMA, Monika. Kernel in Operating System [online]. 05.05.2022 [cit. 2022-11-09]. Dostupné z: https://www.includehelp.com/operating-systems/kernel.aspx

[15] Prehľad edícií Windows 10 [online]. 27.12.2021 [cit. 2022-11-15]. Dostupné z: https://melisko.webnode.sk/news/software-a-zakladne-pojmy-operacnych-systemov/

[16] BORKO, Martin. Čo je to Linux a aké má výhody a nevýhody v porovnaní s Windowsom 10? [online]. 17.09.2020 [cit. 2022-11-17]. Dostupné z: https://vosveteit.zoznam.sk/co-je-to-linux-a-ake-ma-vyhody-a-nevyhody-v-porovnani-s-windowsom-10/

[17] How the Linux OS Was Announced to the World in 1991 [online]. 25.04.2011 [cit. 2022-11-17]. Dostupné z: https://www.flickr.com/photos/methodshop/5654683066

[18] PARKER, Jeff. Active Directory: Guide to Terminology, Definitions & Fundamentals [online]. 29.09.2022 [cit. 2022-11-25]. Dostupné z: https://www.pcwdld.com/active-directory-guide

[19] DUCHOŇ, Jiří. Role a Funkce Windows Server 2016 [online]. 22.06.2018 [cit. 2022-11-25]. Dostupné z: https://jiri-duchon.cz/2-role-a-funkce-windows-server-2016/

[20] ALLEN, Robbie a Alistair G. LOWE-NORRIS, 2005. Active Directory: implementace a správa Microsoft Active Directory. Praha: Grada. ISBN 80-247-0973-2

[21] DNS in Active Directory [online]. 03.7.2022 [cit. 2022-11-25]. Dostupné z: https://infosecwriteups.com/dns-in-active-directory-dcb93b10c3f3

[22] DNS Training Subdomain Example [online]. 20.12.2015 [cit. 2022-11-25]. Dostupné z: https://dnstraining.space/subdomains.html

[23] HUNTER, Laura E. a Robbie ALLEN, 2009. Active directory cookbook: solutions for administrators and developers. 3rd ed. Sebastopol, CA: O'Reilly. ISBN 9780596521103

[24] GILLIS, Alexander S. Web Server [online]. 07.07.2020 [cit. 2022-11-27]. Dostupné z: https://www.techtarget.com/whatis/definition/Web-server

[25] SOUKUP, Ondřej. Co jsou skupiny zásad (Group Policy) [online]. 18.09.2009 [cit. 2022-12-05]. Dostupné z: https://www.techtarget.com/whatis/definition/Web-server

[26] BOUŠKA, Petr. Active Directory komponenty – domain, tree, forest, site [online]. 08.02.2008 [cit. 2022-12-10]. Dostupné z: https://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/

[27] STANEK, William R., 2009. Active Directory: administrator's pocket consultant. Redmont: Microsoft Press. ISBN 9780735626485

[28] O DOMÉNÁCH A DNS [online]. 2021 [cit. 2022-12-10]. Dostupné z: https://www.nic.cz/page/312/o-domenach-a-dns/

[29] JEBAVÝ, Josef. Proč je Linux bezpečnější než Windows [online]. 05.8.2020 [cit. 2023-05-10]. Dostupné z: https://cs.joecomp.com/why-linux-is-more-secure-than-windows

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

IP	Internet Protocol, Internet Protocol Address
TCP	Transmission Control Protocol
IPv4/IPv6	Internet Protocol version 4/6
DNS	Domain Name Systém
MAC	Media Access Control
Wi-Fi	Wireless Fidelity
KDC	Key Distribution Center
TGS	Ticket – granting server
SSO	Single Sign – On
PC	Personal Computer
DOS	Disk Operating Systém
IBM	International Business Machines Corporation
QDOS	Quick and Dirty Operating Systém
OS	Operating Systém
GPL	General Public License
BIOS	Basic Input Output Systém
UEFI	Unified Extensible Firmware Interface
MBR	Master Boot Record
GPT	Guid Partition Table
TB	Terabyte
CLI	Command Line Interface
GUI	Graphic User Interface
BSD	Berkeley Software Distribution
Windows NT	Windows New Technology
DHCP	Dynamic Host Configuration Protocol

WSUS	Windows Server Update Services
SuSE	Software und System Entwicklung
LAMP	Linux, Apache, MySQL, PHP
MySQL	My Structured Query Language
PHP	Hypertext Preprocessor
HDD	Hard Disk Drive
SSD	Solid – State Drive
CD	Compact Disc
IT	Information and Communication Technologies
POST	Power on Self-Test
FAT	File Allocation Table
EXT	Extended Filesystem
GRUB	Grand Unified Bootloader
LILO	Linux Loader
SIM	Subscriber Identity Module
SSID	Service Set Identifier
USB	Universal Serial Bus
RAM	Random Access Memory
AD DS	Active Directory Domain Services
LDAP	Lightweight Directory Access Protocol
DNS	Domain Name System
WINS	Windows Internet Naming Service
OU	Organizational Unit
SW	Software
VHD	Virtual Hard Disk
AD	Active Directory

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: NÁZOV PRÍLOHY