Návrh a implementace bezpečné IT infrastruktury

Bc. Ondřej Nemrava

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Ondřej Nemrava**
Osobní číslo:	**A18630**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Návrh a implementace bezpečné IT infrastrukury**
Téma práce anglicky:	**The Design and Implementation of a Secure IT Infrastructure**

Zásady pro vypracování

1. Specifikujte požadavky na infrastrukturu dle zadavatele.
2. Zpracujte návrh síťové infrastruktury dle zadání v bodě 1.
3. Proveďte implementaci v testovacím prostředí.
4. Ověřte funkčnost implementace řešení – proveďte penetrační test infrastruktury pro ověření monitoringu a ochranných funkcí.
5. Zpracujte implementační manuál a průvodce pro správce.

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

Seznam doporučené literatury:

1. BROOKS, R. R. Introduction to computer and network security: navigating shades of gray. Boca Raton: CRC Press, c2014. ISBN 978-1-4398-6071-7.
2. SELECKÝ, Matúš. *Penetrační testy a exploitace*. Brno: Computer Press, 2012. ISBN 978-80-251-3752-9.
3. *Sys Admin: the journal for UNIX and Linux systems administrators*. San Francisco: CMP Media LLC. ISSN 1061-2688.
4. BINNIE, Chris. *Linux Server security: hack and defend*. Indianapolis, Indiana: Wiley, [2016].
5. KIM, Peter. *Hacking: praktický průvodce penetračním testováním*. Přeložil Jan POKORNÝ. Brno: Zoner Press, 2015. Encyklopedie Zoner Press. ISBN 978-80-7413-313-8.

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

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/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- 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/bakalářské 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 13.08.2020

Ondřej Nemrava v.r
podpis diplomanta

ABSTRAKT

Diplomová práce se věnuje tématu navržení a následné implementaci informační infrastruktury a jejího následného testování z hlediska bezpečnosti. V první části se zaměřuje na teoretický plán výstavby IT prostředí a použitých prvků a základním postupům. Ve druhé, praktické části, se věnuje samotné implementaci IT infrastruktury a následným penetračním testům pro ověření bezpečnosti produktu.

Klíčová slova: IT, infrastruktura, penetrační testy, bezpečnost

ABSTRACT

Master thesis deals with design and implementation of an IT infrastructure subsequently covering penetration tests concerning the infrastructure security. In the first part of the thesis, it focuses on planning the infrastructure, used technologies and basic processes. In the second part, which is practical, it deals with the implementation itself and follow-up penetration tests to verify product´s security.

Keywords: IT, infrastructure, penetration tests, security

Tímto bych chtěl poděkovat vedoucímu mé práce Ing. Davidu Malaníkovi, Ph.D., za odborné vedení diplomové práce, poskytnutí konzultací, rad a materiálových podkladů. Dále bych chtěl poděkovat Petru Švorčíkovi za poskytnutí hardwarového vybavení pro uskutečnění a zpracování diplomové práce. Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Ačkoli se informační svět dělí na nespočet odvětví a zaobírá se různými, někdy i naprosto odlišnými tématy, jedním ze základních kamenů stále zůstává samotná infrastruktura, která dovoluje jedincům nebo i rozsáhlým korporacím fungovat v dnešním informačním věku. Infrastruktura jako taková zastupuje páteř doménových sítí a poskytuje služby a zdroje vyžadované pro správný chod společnosti. Skládá se ze všech složek IT prostředí, které jsou mezi sebou propojeny. První částí je již zmíněný hardware neboli fyzické prostředí, dále pak software, což jsou systémy, aplikace a další nástroje. Součástí jsou taktéž síťové prvky a vybavení, nebo zařízení, která vyžadují IT podporu či monitoring. Dále pak navazují již konkrétní služby, které poskytuje infrastruktura v podobě uživatelských databází, záloh, aktualizací, připojení, sdílení souborů a další.

Již od počátků seznamování se s počítačovým světem jsem měl vždy blízko k hardwarové stránce IT světa. Také proto jsem si zvolil toto téma, které navazuje na základní fyzickou implementaci, a i v praxi je mým oborem zájmu. Navíc považuji toto téma jako rozšíření dosavadních znalostí a zhodnocení jejich získání v praxi, což může být základem pro získání dalších zkušeností a vzdělání v oboru informačních technologií, bezpečnosti a managementu. Práce nebude zcela cizí i nezainteresovaným čtenářům, neboť se s tímto tématem setká většina lidí pohybujících se v korporátním světě, kde nelze bez již zmíněné infrastruktury existovat. V rámci práce taktéž využijeme referenční model OSI, který nám slouží jako základní diagnostický nástroj a rozdělení počítačových sítí, neboť budeme propojovat různé systémy a je nutné zajistit jejich funkčnost ve všech vrstvách. V teoretické části práce se budeme zabývat plánem, použitými zdroji a prvky infrastruktury. Popíšeme si základní postupy a pravidla pro tvorbu jednotlivých součástí práce a zahrneme krátkou dokumentaci využitých produktů a software pro penetrační testy, kterými budeme kontrolovat bezpečnost. V praktické části pak provedeme samotnou implementaci navržené struktury, její otestování a ověření bezpečnostní integrity. Dále pak bude zahrnovat vizuální dokumentaci jednotlivých kroků průběhu tvorby IT infrastruktury. Taktéž zahrneme vizuální dokumentaci penetračních testů a jejich výsledky.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ TECHNOLOGIE

K vytvoření IT infrastruktury je možné přistoupit dvěma způsoby. První možností je implementace celého systému na fyzické vrstvě, což znamená využití hardwaru pro každý prvek v síti a jeho následného osazení požadovaným softwarem. Každý fyzický server zahrnuje procesor, paměti, pevné disky, síťové připojení a operační systém. Nevýhody jsou velké prostorové zatížení kvůli všem zahrnutým komponentům. Kdežto naopak virtuální zpracování infrastruktury požaduje nejméně jeden fyzický server, který má dostatečné parametry pro simultánní běh několika virtuálních strojů (dále již jen „VM“), není podmínkou, že celý systém musí běžet na jednom fyzickém serveru, ale odvíjí se od náročnosti celého systému. Na již zmíněný fyzický server se instaluje prostředí a serverové zdroje se virtualizují a sdílejí pro všechny VM nainstalované na serveru. Z virtualizačních systémů jsou nejznámějšími zástupci Microsoft Hyper-V, VMware vSphere, Oracle VM VirtualBox a další, které jsou pak nainstalovány a poskytují služby a prvky potřebné k funkčnosti takového virtuálního systému. Výhodou takového zpracování je v první řadě finanční stránka, kde není nutné mít desítky hardwarových prvků, ale stačí omezené množství a virtualizační software. Dále pak menší náročnost na serverové prostory, chlazení systémů a servisní výdaje. Dalšími výhodami virtuálních serverů je rychlost obnovy po pádu serveru, či útoku na systém, jednodušší přenositelnost, rozšiřitelnost, implementace bezpečnostních opatření. Nevýhodou jsou pak nutné nákupy licencí a expertíza v oblasti virtualizace a serverů zainteresovaných pracovníků. [1]

1.1 Požadavky na infrastrukturu

Při zadání práce byla zvolena následná infrastruktura s dalšími prvky, které nebyly zmíněny, nicméně jsou nezbytnými k funkčnosti a sestavení systému.

1.1.1 Servery

Základním prvkem jsou zde servery, které byly zadány:

- Doménový kontroler (dále už jen DC)
- Webový server
- VPN server
- Emailový server
- Síťové úložiště (File server)

- Server pro tiket systém (Aplikační server)

Dodatečné servery, které byly zvoleny pro plnou funkčnost infrastruktury:

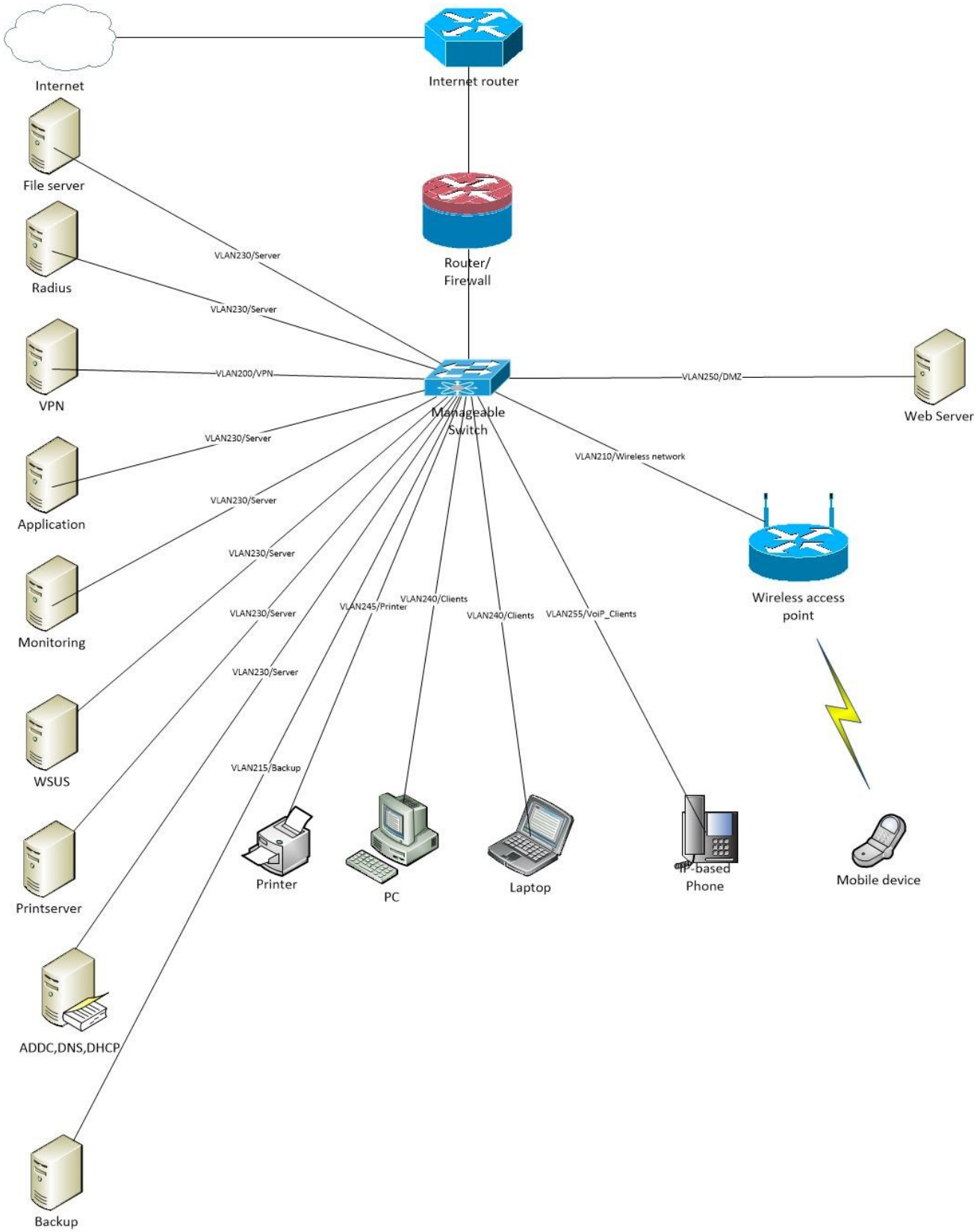
- DHCP server
- DNS server
- Monitoring server
- WSUS server
- Tiskový server
- Radius server
- Zálohovací server

1.1.2 Klienti

Dle zadání implementujeme desktopové počítače, laptopy a síťové tiskárny (které ovšem budou zpracovány pouze teoreticky – dle zadání) a mobilní telefony.

1.1.3 Síťová infrastruktura

Síťová infrastruktura je zvolena dle požadavků na ochranu proti ransomwaru. Dále je také implementováno rozdělení do VLAN kvůli možnostem rozdílných politik a pravidel. Zařízení mají mít možnost cestovat po celém světě a stále mít možnost připojit se k DC. Taktéž může uživatel neboli zaměstnanec pracovat na vlastním zařízení ve firemní síti (BYOD).



Obrázek 1 - Topologie sítě

1.2 Virtuální prostředí a hardware

Pro tuto práci byl zvolen virtuální přístup k tvorbě infrastruktury. Neboť pro funkční infrastrukturu ve fyzické podobě by bylo potřeba nemalých finančních prostředků a volných prostor. Dále taktéž množství prvků L1 vrstvy (fyzická první vrstva OSI modelu) a dalších L2 prvků pro zprovoznění síťové infrastruktury požadovaných serverů, navíc plně vyhovuje zadání práce.

1.2.1 Fyzický server

Prostředky pro celý systém poskytuje jeden ESXi server HP Proliant DL360 G7, který je osazen 24 GB ECC pamětí, Intel Xeon E5620 2.40GHz serverovým procesorem, který poskytuje 8 logických jader. Obsahuje čtyři fyzické NIC karty. Úložná kapacita serveru je 1,9 TB. Server provozuje veškeré VM a taktéž virtuální switch. Pro dosažení a udržení 100 % serverového provozu byly elektrické zdroje (PSU) připojené k různým elektrickým 230 V zásuvkám. Obvyklá a doporučovaná praxe je v tomto případě připojit jeden ze zdrojů k pevné síti a druhý k UPS zařízení, které při výpadku dodávek elektrického proudu zvládne systém udržet v provozu dobu dostatečnou k obnovení standartní dodávky napájení, nebo nalezení jiného dlouhodobějšího zdroje, jako jsou například dieselové agregáty apod. [2]

1.2.2 Virtualizační software

Pro virtualizace je použit již zmíněný VMware Vsphere, který nejlépe zaštítí tvorbu VM pro naše účely. Výhodou je taktéž volně stažitelná verze pro evaluaci, kterou poskytuje samotný VMware, tudíž není nutné platit za licenci a software není omezen ani po uběhnutí této doby natolik, aby byla tato práce ohrožena, či znemožněna. Omezením je hlavně nemožnost používat vCenter a spojovat vícero hostů (fyzických serverů, kde běží VMware) do clusteru (cluster = „seskupení stejných prvků“). Konkrétně byla použita verze VMware Vsphere 6.0 společně s Vsphere klientem nainstalovaným na fyzický počítač pro nastavení, úpravy a další. [4]

1.2.3 Síťové prvky

Pro účely plné funkčnosti dle sítě dle určených požadavků byl zvolen deseti portový L3 switch od Mikrotiku, konkrétně RB2011UiAS s podporou VLAN tagování. Mikrotik přijímá internet pomocí CAT 5E kabelu od místního providera a následně zprostředkovává oddělené testovací prostředí pro implementaci, provoz a testování infrastruktury. V rámci prostředí

RouterOS poskytuje taktéž uspokojivé řešení ověřování uživatelů pro VPN server, nicméně tato možnost nebyla využita. Dále zprostředkovává síťový firewall, který již není dále řešen samostatným síťovým zařízením. Možnosti DHCP a DNS serveru v rámci Mikrotik switche nejsou využity, neboť zpracování probíhá na DC serveru, stejně jako sledovací služby. Firewall nicméně bude využit přímo v rámci Mikrotiku. Následně jsou využity možnosti VMware softwarové virtualizace a v prostředí Vsphere jsou vytvořeny další virtuální síťové prvky v podobě vSwitch zařízení. Pomocí Mikrotiku taktéž oddělujeme DMZ (demilitarizovanou zónu) pro služby, které by měly být dostupné mimo naši interní síť od zbytku infrastruktury. [5]

1.3 Serverová implementace

Většina našich serverů je postavena na jádře Windows, konkrétně Windows Server 2019. Jedná se o neaktivované verze Windows. Pro naše uzavřené testovací prostředí nepotřebujeme verze aktivovat, jelikož nás neaktivovaný systém neomezuje.

Avšak mezi servery najdeme i Linux kernel, na kterých běží konkrétně VPN server, Radius server a Monitoring server.

1.3.1 Domain Controller (DC)

Doménový kontroler, jako jediný obsahuje vícero služeb a funkčností v jednom VM. Poskytuje ADDS (Active directory domain services). Taktéž přiděluje dynamické IP adresy a poskytuje DNS. Spravuje doménu a poskytuje pravidla, politiky pro celou infrastrukturu.

1.3.2 Webový server

Webový server poskytuje přístup k webové stránce, na kterou je možné přistupovat z vnější sítě, proto je vhodné server oddělit od ostatní infrastruktury. Tudíž je server v tzv. DMZ (demilitarizované zóně) což znamená, že je na něj povolen přístup pomocí kupříkladu portu 80 a v případě napadení je firewallem oddělen od zbytku infrastruktury, tudíž nehrozí rozšíření viru, nebo jiného problému. V případě ataku poté stačí obnovit pouze tento webový server, bez obav o ostatní prvky systému.

1.3.3 Aplikační server

Poskytuje a funkce pro uživatele systémové infrastruktury, v případě společnosti lze mluvit o různých aplikacích, které jsou dostupné pro všechny uživatele, jako například docházkový

software. Náš aplikační server poskytuje ticketovací systém. Což je systém pro zadávání IT požadavků. Výhodami jsou zpětně dohledatelné požadavky, archivované žádosti o administrátorská práva, statistiky a podobně. Na serveru funguje open-source ticketovací systém od osTicket který je zdarma a poskytuje dostatečné zázemí pro naše využití.[6]

1.3.4 Backup server (záložní)

Záložní server poskytuje obnovitelné zálohy celého systému, kde je možné využít mnoha zálohovacích řešení a taktéž dle velikosti systému zálohovat servery, nebo i klienty. Zálohy budou probíhat pouze na serverech, neboť zálohování klientů by vyžadovalo mnohem vyšší kapitál a veškerá důležitá data by měli mít navíc uživatelé uloženy na fileserveru. Jako zálohovací řešení budeme využívat zkušební verzi Veeamu, která je pro nás dostupná na 30 dní zdarma. Zároveň poskytuje komplexní řešení pro fyzické i virtuální servery. Poskytuje ochranu proti Ransomware a umožňuje periodicky zálohovat různé operační systémy, navíc umožňuje rychlou a jednoduchou obnovu dat. [7]

1.3.5 Tiskový server

Server pro síťový tisk bude pod záštitou Windows Server 2019, kde poskytuje naprosto ideální prostředí pro sdílení tiskáren, statistiky tisku, možnosti monitoringu. Vzhledem k pouze teoretickému zpracování tiskového klienta, nebude mít nainstalované aktivní klienty, pouze prostředí nachystané pro případné připojení fyzických tiskáren.

1.3.6 Monitoring server

Bude poskytovat sledovací a statistické služby pro celý systém. Postaven na Linux kernelu bude využívat open-source multiplatformového systému Zabbix. Který nabízí veškeré potřebné služby od sledování síťové aktivity, fyzických serverů, VM, cloudových řešení, aplikací, služeb, webu, úložných zařízení, Java aplikací, databází, telefonních přístrojů a zabezpečení. [8]

1.3.7 VPN server

Taktéž funkční na Linuxovém základu, poskytuje možnost připojení zařízení do interní sítě pomoci zabezpečeného VPN tunelu z jakéhokoli místa na světě, díky ověřování vůči dedikovanému Radius serveru. Využívá volně dostupné řešení od OpenVPN. Které poskytuje management v podobě terminálového prostředí, nebo i webové GUI. Samozřejmostí je funkčnost pro cross-platform zařízení. [9]

1.3.8 Radius

Plné znění zkratky Radius zní Remote Authentication Dial-In User Service, což je software a serverový a klientský protokol, který umožňuje hlavnímu serveru ověřovat a autorizovat přístup vzdáleně přistupujícím uživatelům k systému, či databázím, které se nacházejí v interní síti. Poskytuje vyšší úroveň zabezpečení infrastruktury, díky udržovaní centrální databáze uživatelů, které je dostupná pro všechny vzdálené přístupové servery, což je spravováno lokální politikou na centrálním serveru. V našem případě bude poskytovatelem Radius služeb samostatný Windows server. [10]

1.3.9 WSUS server (aktualizace)

Neboli Windows Server Update Services, je služba, která zajišťuje softwarové aktualizace v rámci operačních systémů Microsoft Windows. Pomocí samostatného aktualizačního serveru jsme schopni korigovat uvolňování aktualizací do firemní sítě. Výhodou WSUS serveru je omezení vytíženosti internetové linky, neboť si může každé zařízená ve firemní síti stáhnout aktualizace z lokálního server, a tudíž nevyužívá šířku pásma internetové linky. [11]

1.3.10 Datový server (fileserver)

Posledním ze serverů je síťové úložiště, které poskytuje prostor pro důležitá data uživatelů a umožňuje jejich dostupnost napříč firemní infrastrukturou. Přístupy pro jednotlivé složky jsou řešeny pomocí práv v Active Directory na našem DC. Zároveň je zvolen diskový prostor pro jednotlivé složky, čímž je vytyčen objem dat pro jednotlivé úseky, které je možné ukládat a zároveň zálohovat.

1.4 Implementace klientů

Dle zadání se budeme věnovat implementaci klientů, a to v podobě pevných počítačů, které budou zpracovány ve virtuální podobě a notebooku ve fyzické podobě. Virtuální desktopy leží na ESXi stroji na samostatných VM. Využívají verzi Windows 10 a vztahují se na ně veškeré politiky a pravidla ADDS. Laptop je připojen fyzicky ke switchi a funguje naprosto stejně jako již zmíněné VM a funguje taktéž na Windows 10. Ostatní klienty, jako jsou síťové tiskárny VOIP telefony a mobilní přístroje, zpracováváme jen teoreticky. Ve firemním prostředí je dle zadání požadována možnost BYOD (Bring your own device, neboli

umožnění zaměstnancům pracovat ve firemní síti na vlastním stroji). Z bezpečnostních důvodů málokdy v praxi využívaná technika. [12]

2 OVĚŘENÍ FUNKČNOSTI INFRASTRUKTURY A PENETRAČNÍ TESTY

Další důležitou součástí výstavby firemní infrastruktury, je následná kontrola funkčnosti a plné operační schopnosti celého systému stejně jako bezpečnostní testy neboli penetrační testy, které napomohou odhalit bezpečnostní nedostatky a možné způsoby napadení systému.

2.1 Hledání slabých míst v infrastruktuře

Při hledání slabých míst v infrastruktuře, čímž je myšlena infrastruktura síťová, ověříme sniffing, dále zamezíme vystavení falešného DHCP a DNS serveru a následně taktéž DNS sniffing a taktéž vzdálený přístup do síťových prostor a datových složek.

2.1.1 Network sniffing

Pro potřeby „síťového čmuchání“ jak by se dal přeložit anglický název, použijeme Wireshark, což je opensource software naprogramovaný pro analyzování síťových protokolů a provozu, umožňuje použití na distribucích Linuxu, nebo Windows a poskytuje množství sledovacích prostředků, jakož jsou: [3]

- Analýza VOIP
- Prohlížeč paketů
- Inspekce protokolů
- Aktivní dekomprese gzip souborů
- Export logů a dat do XML, CSV, textu a Postscript

2.2 Penetrační testy

Penetrační testy nám poskytne linuxová distribuce KALI, kde oskenujeme síťové porty, čímž eliminujeme možnost nabourání do systému pomocí portů, které by zůstaly otevřeny případným útočníkům, ale přitom by nebyly funkčně využívány. Dále provedeme SQL injection pomocí SQLMap, kde lze pomocí SQL „vsunutí“ žádosti do protokolu získat uživatelské údaje, či změnit oprávnění pro uživatele. Dále je nutné provést testy uživatelského zabezpečení, převážně hesel, a to pomocí brute-force útoku, který nám poskytne Hydra. Penetrační testy budeme dělat jednak externě a dále poté interně. Díky tomu ověříme zabezpečení vůči útokům zvenčí i z vnitřní části sítě. [13]

II. PRAKTICKÁ ČÁST

3 PŘÍPRAVA ESXI

Základem pro celou praktickou část diplomové práce je zprovoznění hardware vybavení, které poskytuje zdroje pro veškerou virtualizaci našich serverů a síťových zařízení. Nejprve je nutné osadit server dostatečnou kapacitou HDD pro úložné prostory virtuálních serverů. Jak již bylo zmíněno v teoretické části, jedná se o ESXi server HP Proliant DL360 G7 využívající 24GB paměti RAM, osazen procesorem Intel Xeon E5620 2.40GHz o 8 logických jádrech. Diskové pole tedy obsahuje 10 pozic pro disky, které všechny využíváme a pomocí deseti SAS HDD disků dosahujeme finální datové velikosti využitelného pole činícího zhruba 1,9Tb prostoru pro virtualizaci a úložné prostory.

3.1 Instalace Vmware

Pro práci je zvolena Vsphere Server verze 6.0 v evaluační kopii, které byla stažena z oficiálních stránek VMware ve formátu virtuálního disku (ISO). Následně byl vložen USB flash-disk do interního USB portu na základní desce serveru o doporučené minimální velikosti 16GB. Dále pomocí příkazové řádky, nebo opensource programu Rufus a jemu podobným vytvoříme bootovatelné médium v podobě flash disku, nebo CD/ROMu (v našem případě USB) a nabootujeme z něj ESXi instalaci. Po načtení instalace projdeme licenční ujednání (potvrdíme klávesou F11) a následně zvolíme naše již připojené USB na základní desce serveru. Je důležité zvolit heslo pro uživatele root, které si budeme pamatovat, ale zároveň zamezí fyzicky přítomným osobám u serveru jej zjistit a provádět nechtěné změny v našem systému. Následuje samotná instalace, která v závislosti na HW trvá zhruba 15 minut. Po dokončení instalace odpojíme instalační USB disk a restartujeme hosta. Po opětovném naběhnutí serveru zvolíme v boot sekvenci naše nově nainstalované USB prvním zařízením.[14]

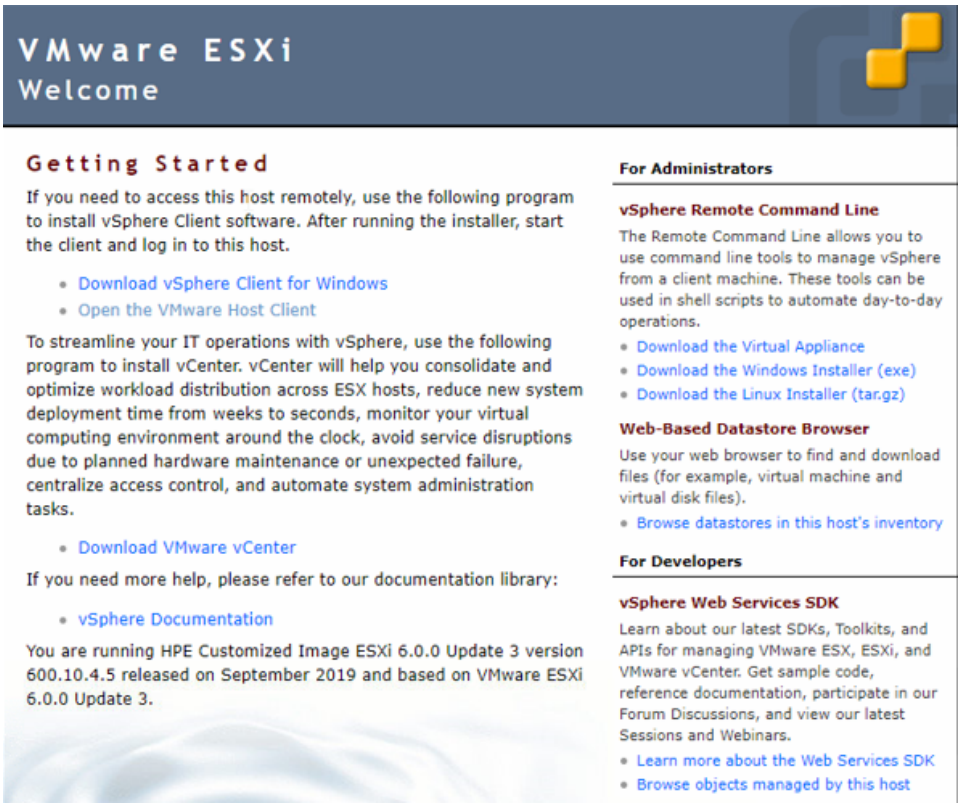
3.2 Diskové pole

Server je osazen 10 fyzickými disky. Pro naše využití potřebujeme pouze jeden RAID, kdy se pomocí klávesy F10 dostaneme ke konfiguraci diskového pole. Ze všech disků vytvoříme logickou RAID jednotku. V praxi existuje vícero typů RAID. RAID (Redundant Array of Independent Disks) je způsobem operování s více než jedním pevným diskem jako jednou logickou jednotkou, a tudíž poskytuje vyšší odolnost systému vůči výpadku, či zániku jednoho z disku v poli. Vybereme možnosti RAID 5, který systému umožňuje rozmisťovat

data na všechny disky v poli a zvládá selhání jednoho disku, kdy při výměně proběhne dopočet originálních dat.

3.3 Prvotní spuštění systému

Při prvním spuštění spustí systém automatickou konfiguraci, během které použije výchozí nastavení pro úložná zařízení a síť (DHCP konfigurace sítě a formátování interních disků do formátu VMFS, který umožňuje uložení virtuálních strojů). Dalším krokem je nastavení síťového přístupu k našemu hostu. Do doby, než budeme mít nakonfigurovanou síť, se k serveru připojíme napřímo pomocí ethernetového kabelu a statické IP adresy kterou nastavíme manuálně ve VMware konzoli. Následně se můžeme pomocí zadané IP adresy k serveru připojit (v našem případě 192.168.220.2) a přihlásit se pomocí uživatelského jména a hesla zvoleného při instalaci. Pro Vsphere verze 6.0 a nižší je možné nainstalovat lokálního klienta, nicméně pro novější verze je již potřeba využívat webové prostředí. Nyní se však budeme zaobírat základním nastavením L3 switche.



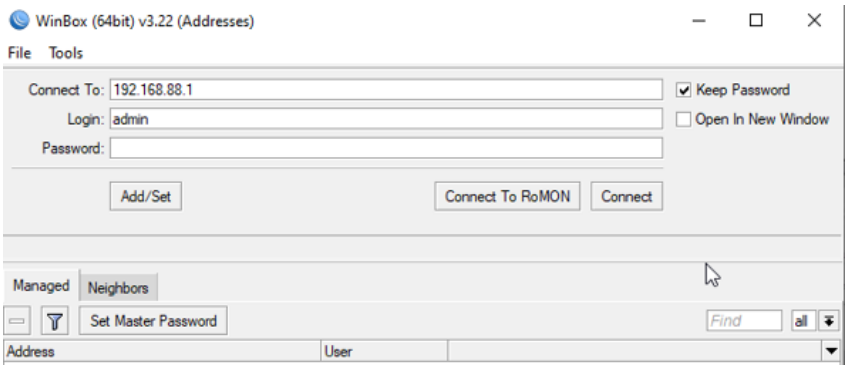
Obrázek 2 - Vsphere Console

4 ZÁKLADNÍ KONFIGURACE SÍTĚ A PRVNÍ VM

Jak již bylo zmíněno v teoretické části, pro síťové potřeby budeme využívat L3 Mikrotik switch RB2011UiAS, který nám umožní routing mezi vícero Vlany a zároveň poskytne základní Firewall pro naši síť.

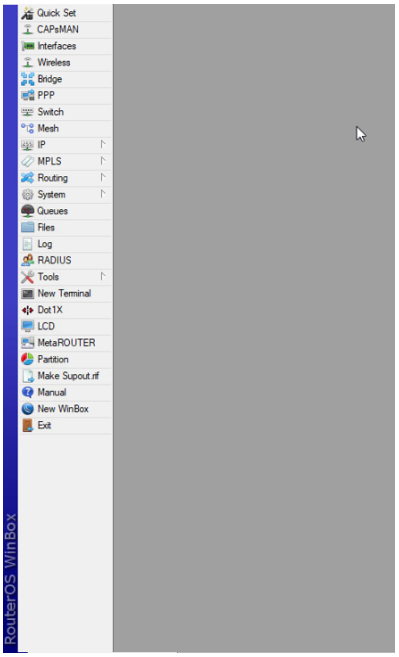
4.1 Prvotní konfigurace Mikrotiku

Pro konfiguraci se k zařízení připojíme pomocí ethernetového kabelu (lze zvolit libovolný port na switchi). Defaultní IP adresa zařízení nalezneme na spodní straně zařízení. Pro naše potřeby použijeme 64bitovou verzi aplikace Winbox, díky které nemusíme využívat webové rozhraní, ale poskytuje přehlednější podobu konfiguračního prostředí RouterOS. Winbox je přímo dostupný z oficiálních stránek Mikrotik. || https://mikrotik.com/download || Software není nutné instalovat a po spuštění pouze zadáme naši defaultní adresu, která je 192.168.88.1 a přihlásíme se pomocí předdefinovaného administrátorského účtu admin (bez hesla). Lze se samozřejmě přihlásit i pomocí mac adresy zařízení, které lze najít v sousedících zařízeních.



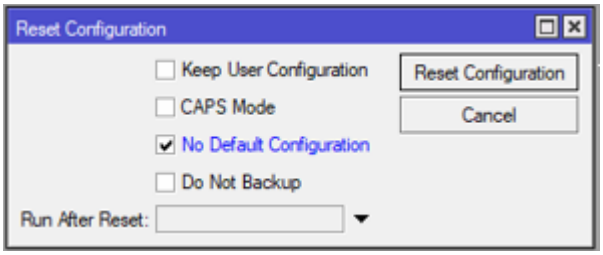
Obrázek 3 - Winbox Login

Tímto se dostaneme do konfiguračního prostředí zařízení. Které díky Winboxu vypadá u všech zařízení Mikrotiku prakticky identicky a je proto snazší se v něm orientovat.



Obrázek 4 - Mikrotik Menu

Mikrotik dodává svoje SOHO zařízení s předpřipraveným nastavením, které ovšem nevyužijeme a zbytečně by nám následně ztěžovalo práci a přehlednost projektu. Tudíž v menu vybereme položku System, která nám nabídne mimo jiné možnost Reset Configuration, což nám umožní vyresetovat zařízení a zrušit veškeré předem konfigurované nastavení. Je nutné zakliknout kolonku No default configuration a pak již jen stačí zvolit Reset Configuration.



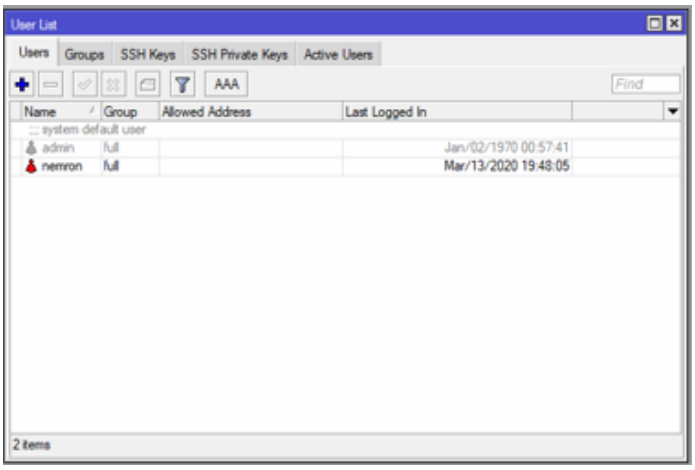
Obrázek 5 - Mikrotik Reset Configuration

Po restartu zařízení se opět přihlásíme pomocí Winboxu. Nyní již „čistý“ Mikrotik můžeme začít konfigurovat.

4.1.1 Zabezpečení L3 switche

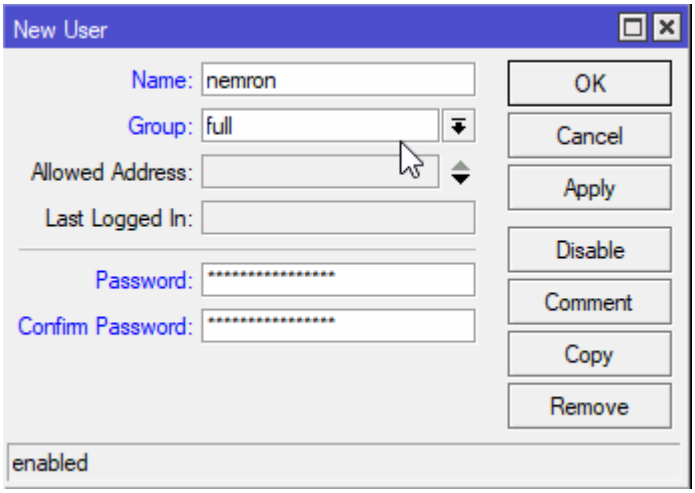
4.1.1.1 Změna administrátorského účtu

Před připojením zařízení do sítě založíme nový přihlašovací účet, pro zamezení přihlášení pod defaultním účtem, který může znát každý, a tudíž zamezení nechtěného přístupu na zařízení. Zvolíme kolonku „Systém“ a dále „Users“, kde již uvidíme defaultní admin účet. [16]



Obrázek 6 - Mikrotik User List

Pomocí plus přidáme nový účet (je možné zvolit vícero typů účtů s jinými právy).

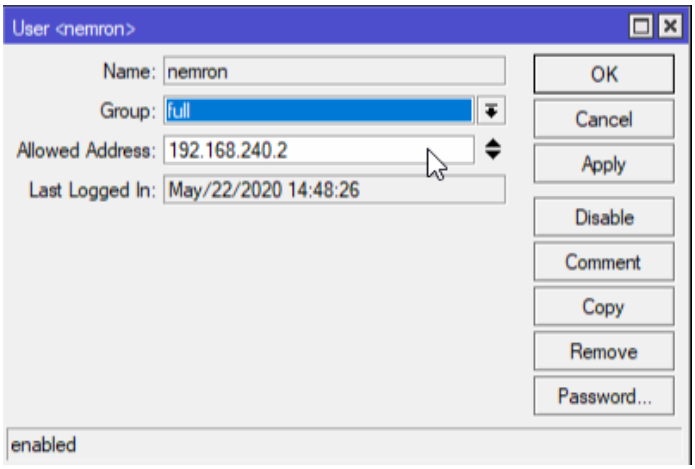


Obrázek 7 - Mikrotik vytvoření uživatele

Zde zvolíme nový název účtu a v rozbalovací liště Group vybereme možnost full, abychom vytvořili administrátorský účet se všemi právy. Je možné zvolit adresu, ze které bude zařízení pod těmito údaji dostupné, nicméně prozatím nevíme, jakou adresu bude mít náš

management počítač, a tudíž doplníme později. Je nutné zvolit dostatečně silné heslo, nejlépe softwarově generované. Nyní pomocí červeného křížku účet admin zakážeme, aby nebylo možné jej nadále využívat. Je nutné se po tomto kroku znovu přihlásit do RouterOS rozhraní.

Následně přiřadíme účtu Allowed Address, což bude jediná IP adresa, odkud se bude moci administrátorský účet nemron připojit k L3 Switchi. Zvolíme adresu 192.168.240.2. Což je rezervovaná statická IP adresa na DHCP serveru pro náš administrátorský počítač. Je možné tuto volbu interpretovat pomocí filtračního pravidla ve firewallu Mikrotiku, a to tak, že povolíme přístup pomocí portů ssh a winboxu (22, 8291) pouze z určitého IP rozsahu, či konkrétní IP adresy. [16]



Obrázek 8 - Mikrotik User settings

4.1.1.2 Zakázání redundantních připojení

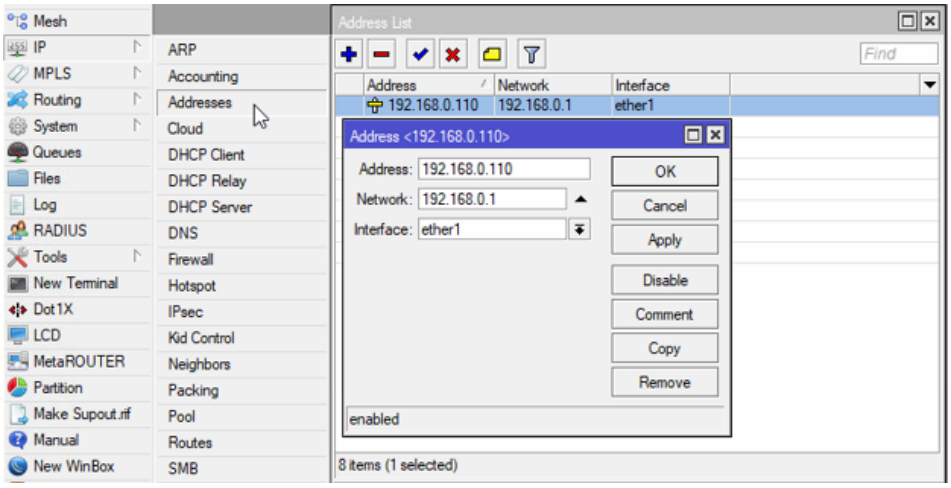
Defaultně jsou povoleny všechny typy připojení jako je telnet, ftp, www a podobně. Pomocí následujícího příkazu, který použijeme v terminálu, který je integrován přímo do RouterOS, zakážeme všechno, co nebudeme využívat. Prvně zjistíme pomocí příkazu: „/ip service print“, které služby jsou spuštěny, a následně znepřístupníme pomocí: „/ip service disable telnet,ftp,www,api,api-ssl“. Což můžeme následně opět zkontrolovat pomocí prvního příkazu. [16]

```
[nemron@MikroTik] > /ip service print
Flags: X - disabled, I - invalid
 #   NAME      PORT ADDRESS                                 CERTIFICATE
 0   telnet      23
 1   ftp         21
 2   www         80
 3   ssh         22
 4 XI www-ssl    443                                         none
 5   api        8728
 6   winbox     8291
 7   api-ssl    8729                                        none
[nemron@MikroTik] > /ip service disable telnet,ftp,www,api,api-ssl
[nemron@MikroTik] > /ip service print
Flags: X - disabled, I - invalid
 #   NAME      PORT ADDRESS                                 CERTIFICATE
 0 XI telnet     23
 1 XI ftp        21
 2 XI www        80
 3   ssh        22
 4 XI www-ssl    443                                         none
 5 XI api       8728
 6   winbox     8291
 7 XI api-ssl    8729                                        none
[nemron@MikroTik] >
```

Obrázek 9 - Mikrotik service printout

4.1.1.3 Nastavení IP adresy

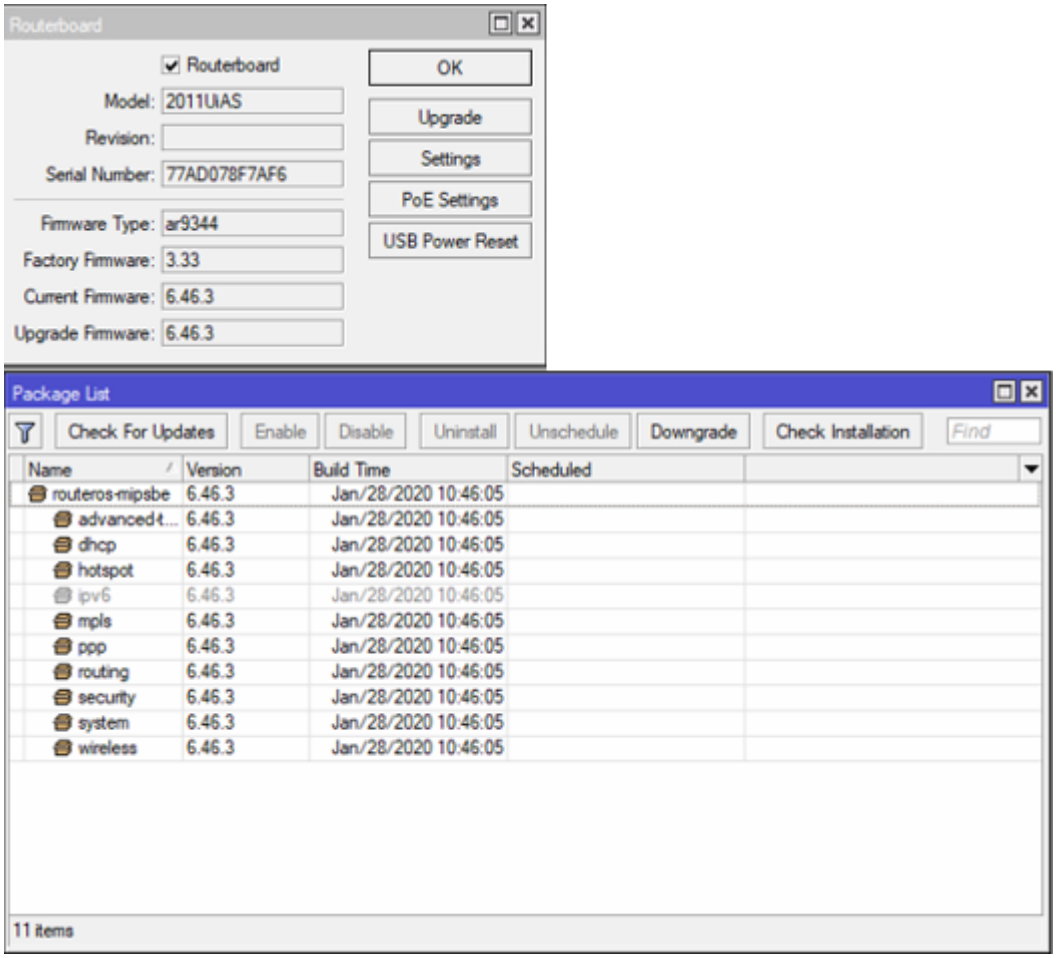
Nežli budeme moci provést připojení routeru k internetu, je potřeba nastavit IP adresu, která nám byla dána od našeho poskytovatele internetu (neboli ISP). V našem případě bude adresa 192.168.0.110. Vybereme možnost IP a následně Addresses, kde pomocí tlačítka plus založíme novou adresu pro port, ke kterému připojíme ethernetový kabel od ISP (například z modemu). Zadáme již zmíněnou adresu 192.168.0.110 do pole Address, což bude konkrétní adresa našeho zařízení. Do pole Network následně zadáme adresu brány do internetu (již dříve zmíněný modem například) a následně zvolíme, ke kterému rozhraní bude adresa přiřazena. V našem případě ether1 (na switchi první ethernetový port).



Obrázek 10 - Mikrotik Router address

4.1.1.4 Aktualizace zařízení

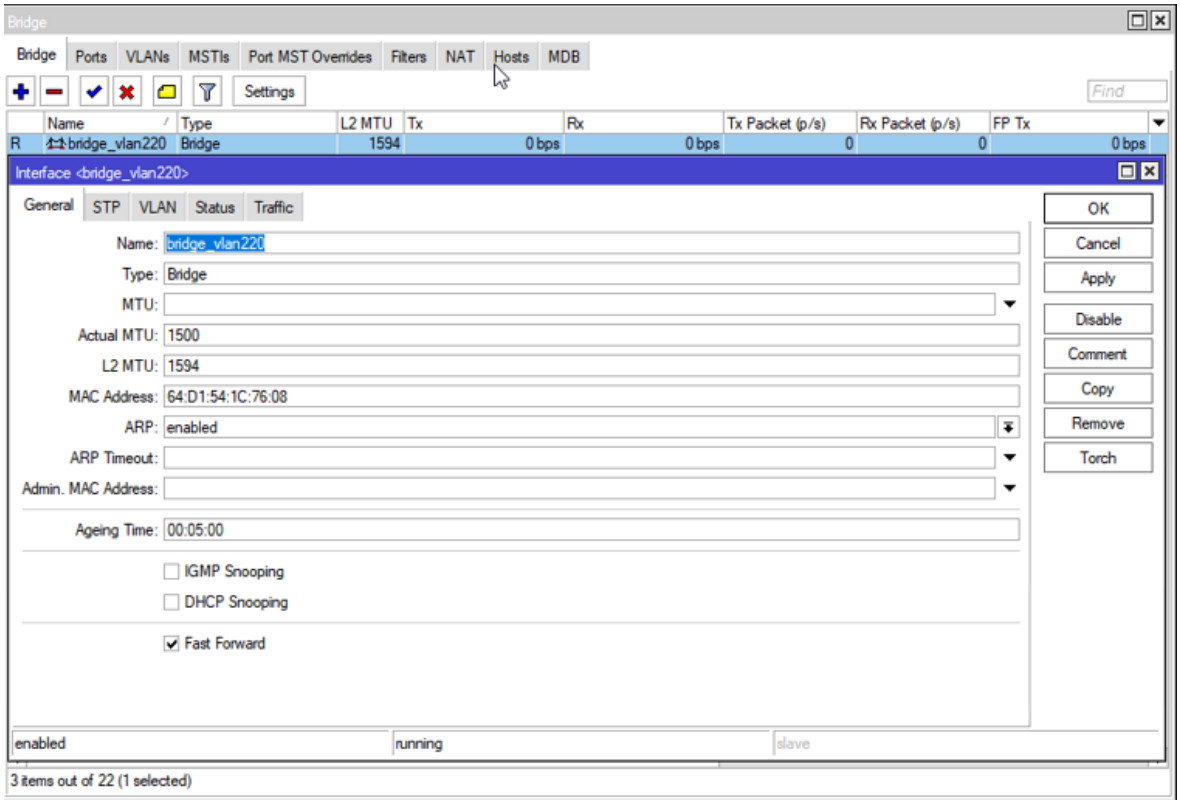
Po přidělení statické IP adresy a připojení zařízení do internetu můžeme provést upgrade zařízení pro získání nových oprav a záplat případných systémových chyb. Zvolíme opět možnost Systém a následně Routerboard, kde je možné díky Upgrade získat poslední možný firmware pro zařízení. Dále ze stejného menu vybereme Package List a provedeme update všech balíčků pomocí Check for Updates. Naše aktuální verze je 6.43.3. Po provedení aktualizace je nutné zařízení restartovat. [16]



Obrázek 11 - Mikrotik aktualizace

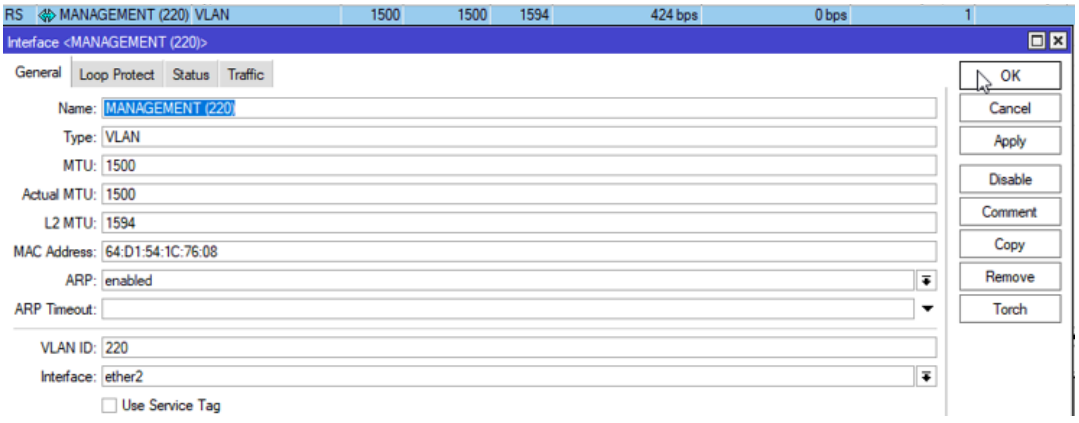
4.1.2 Připojení k ESXi

Nyní nastavíme připojení, abychom měli přístup k ESXi serveru. Vzhledem k běžné praxi nastavíme servisní síť neboli Management network na oddělenou virtuální lokální síť neboli VLAN. Prvně vytvoříme bridge abychom byli schopni následně vytvořit trunkové připojení pro další zařízení. (trunk = „port předávající všechny vlany na další zařízení bez omezení“). V menu Bridge pomocí tlačítka plus založíme nový bridge (v našem případě pojmenujeme bridge_vlan220).



Obrázek 12 - Bridge_vlan220

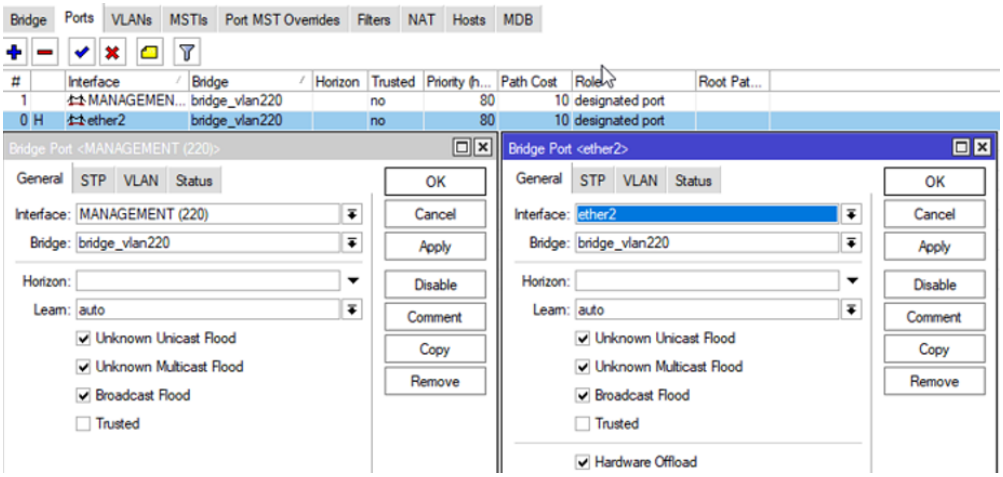
V menu Interface vybereme kolonku VLANs, kde vytvoříme novou VLANu, kterou pojmenujeme MANAGEMENT (220), zvolíme její VLAN ID (u nás 220) a přiřadíme ji ke správnému rozhraní (ether2, které se váže k fyzickému portu číslo 2 na switchi).



Obrázek 13 - Management (220) Interface

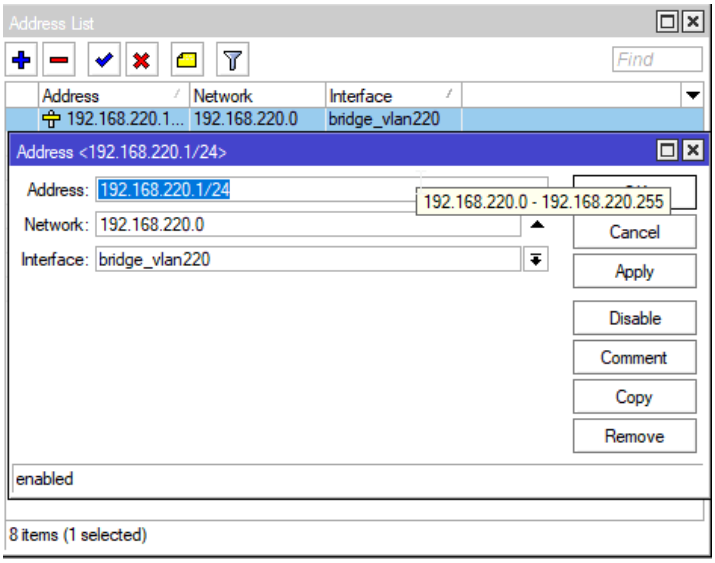
Nyní je potřeba vytvořit porty v menu Bridge/Port, abychom mohli novou Management Vlan přiřadit k dříve vytvořenému bridge_vlan220. Nejprve vytvoříme port pro ethernetový port na switchi a přiřadíme jej k bridge a následně vytvoříme druhý port MANAGEMENT (220)

a taktéž ho připojíme do bridge. Díky tomu přiřadíme oba porty k takzvanému společnému rozhraní a tím se Vlan stane funkční a naše ESXi bude dostupné na zvolené adrese.



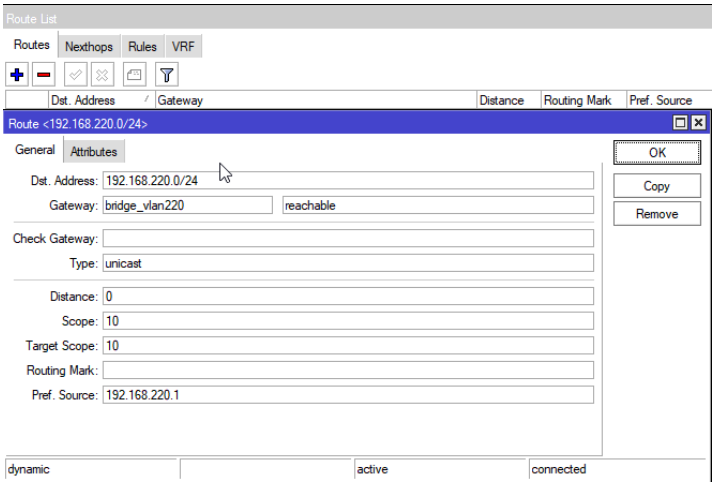
Obrázek 14 - Vytvoření portů pro Management

Ale aby to bylo možné, je potřeba k vytvořené Vlan a rozhraní přiřadit požadované adresní pole a umožnit směrování mezi jednotlivými sítěmi. V menu Address List přiřadíme našemu rozhraní adresu 192.168.220.1/24, která bude následně fungovat jako brána do virtuální lokální sítě (kde /24 značí masku sítě, která lze interpretovat taktéž jako 255.255.255.0) o adresním poli 192.168.220.1 – 192.168.220.255 neboli 192.168.220.0. Dále zvolíme rozhraní ke kterému připojíme náš nový adresní list. Nyní budeme schopni přiřazovat ve Vlan MANAGEMENT (220) IP adresy ať již statické nebo pomocí DHCP serveru.



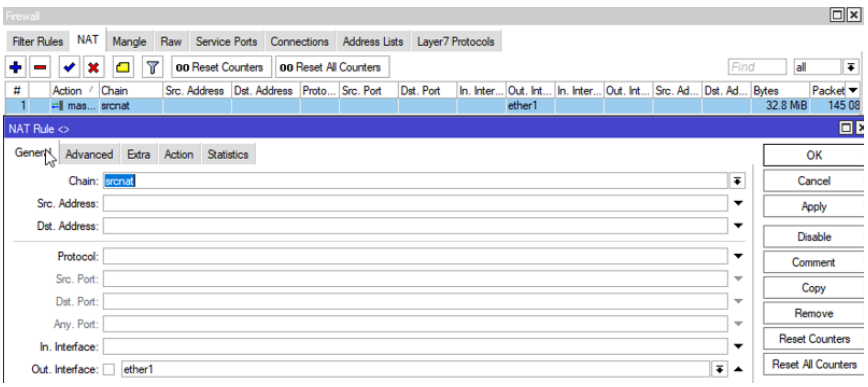
Obrázek 15 - Management adresní pole

Zároveň se nám při vytvoření adres automaticky vygeneruje route (cesta), díky které je naše zařízení schopno směrovat komunikaci.

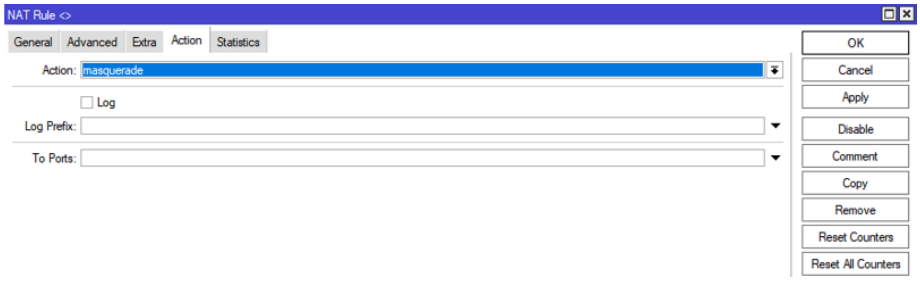


Obrázek 16 - Route 192.168.220.0/24

Posledním krokem pro funkční virtuální síť bude vytvoření pravidla pro překlad adres z vnitřní sítě na vnější IP adresu, neboli díky tomuto pravidlu bude zařízení ve vnitřní síti dostupné z vnější sítě a naopak. Použijeme IP masquerade, což je pravidlo, které všechny adresy v interní síti překládá na jednu veřejnou adresu. Neboli umožňuje několika zařízením funkovat na jedné placené adrese. Pro založení nového NAT pravidla zvolíme menu Firewall/NAT a zde pomocí tlačítka plus vytvoříme nové pravidlo, kde v liště General vyberem v kolonce Chain srcnat a Out. Interface ether1, což je port kam je zapojen vnější internet a v liště Action vybereme již zmiňovanou akci masquerade, bez které by jakékoli zařízení v některé z našich sítích nebylo schopné se dostat na vnější síť.



Obrázek 17 - NAT rule



Obrázek 18 - NAT rule 2

4.2 Založení prvního virtuálního serveru

V této podkapitole vytvoříme první virtuální stroj a na něj následně nainstalujeme server, Posléze budeme tento postup tvorby VM několikrát opakovat, jelikož virtuálních serverů budeme potřebovat několik a budeme se proto odkazovat na tuto část práce abychom se vyhnuli repetitivnímu opisovaní stejného postupu.

4.2.1 Vytvoření VM ve Vsphere

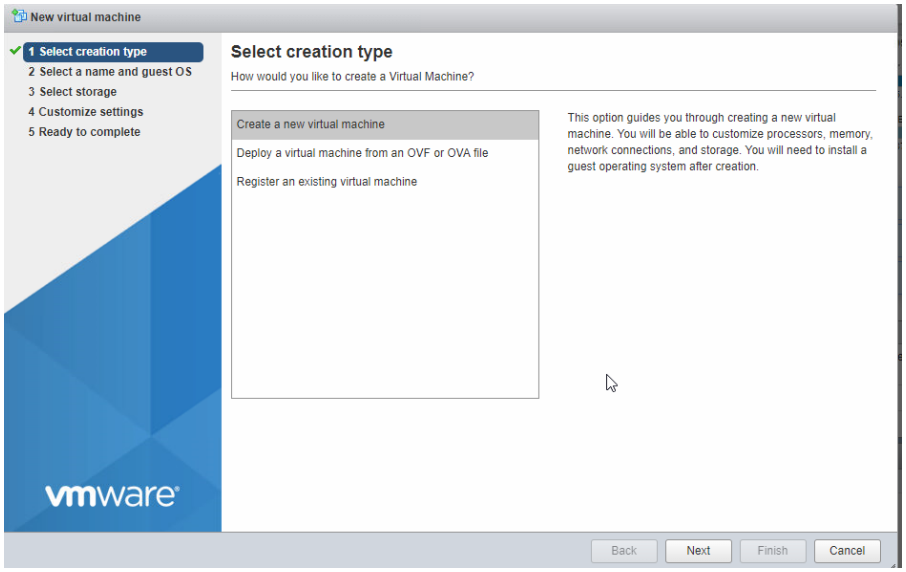
Většinově budeme využívat webový interface, který poskytuje VMware pro konfiguraci a management serverů, nicméně již zmiňovaného Vsphere klienta budeme využívat při konfiguraci virtuálního síťového zařízení, jelikož poskytuje přehlednější možnosti nastavení a orientace.

4.2.1.1 Vytvoření instalačního média

Pro získání instalačního média navštívíme https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019, kde je možné zdarma stáhnout ISO verzi Microsoft Server 2019 pro evaluaci a testování, tudíž není nutné verzi licencovat. Výhodou je již předpřipravený obraz disku, který lze použít k vytvoření instalačního média, nebo vytvoření virtuálního systému přímo ze staženého souboru. Nyní se můžeme přihlásit do webového prostředí na námi zvolené adrese 192.168.220.2 pomocí dříve zadaných údajů při instalaci VMware. [14]

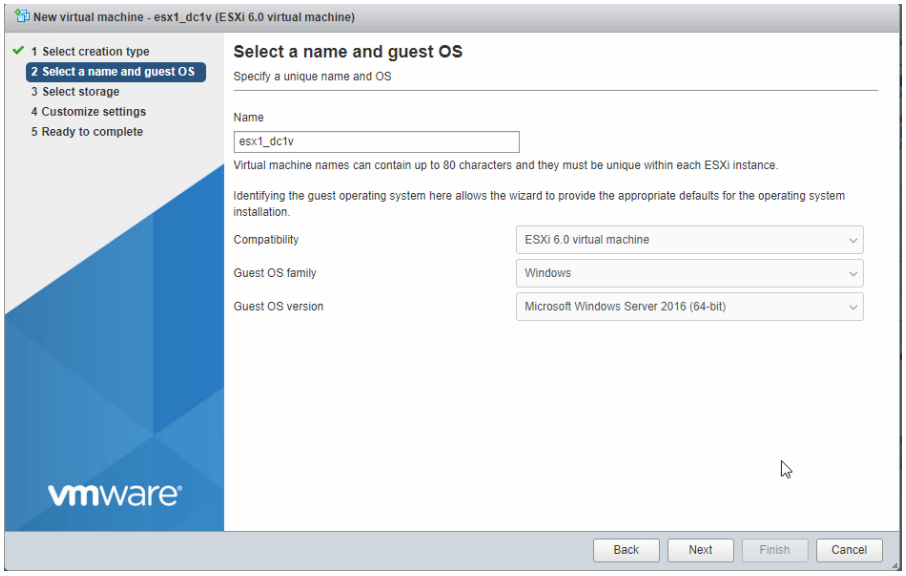
4.2.1.2 Založení VM

Po přihlášení se orientujeme pomocí levé navigační lišty a volíme Virtual Machines a pravým tlačítkem myši otevřeme následné menu, kde vybereme Create/Register VM.



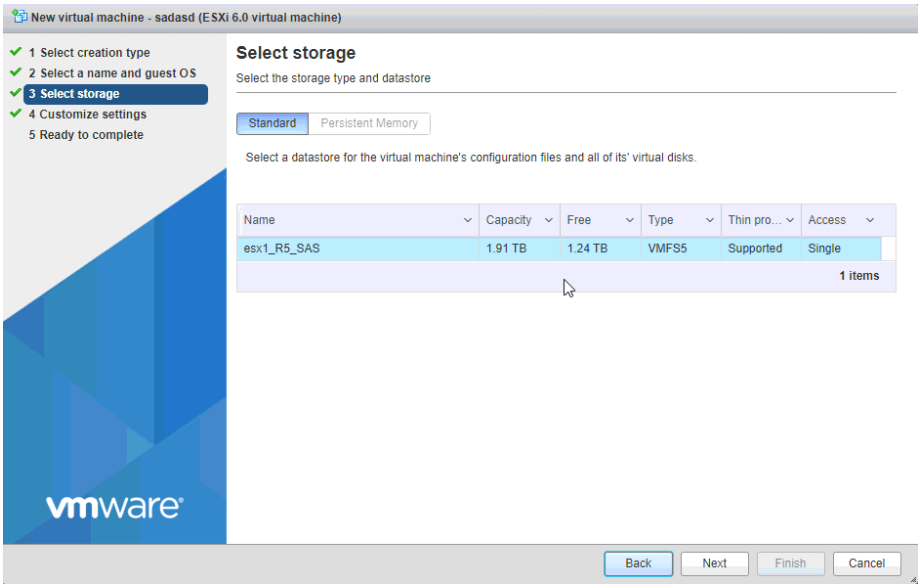
Obrázek 19 - VMware Vytváření dc1v č.1

Dále pokračujeme na další část registrace nového VM pomocí předpřipraveného instalačního průvodce, kde je potřeba zadat jméno virtuálního stroje (většinově název hosta následovaný názvem virtuálního serveru, konkrétně „esx1_dc1v“), vybrat typ operačního systému a následně jeho verzi. Vzhledem k použité verzi Vsphere v nabídce není Windows Server 2019, ale pouze 2016, což je ale ekvivalentní, a proto zvolíme verzi 2016.



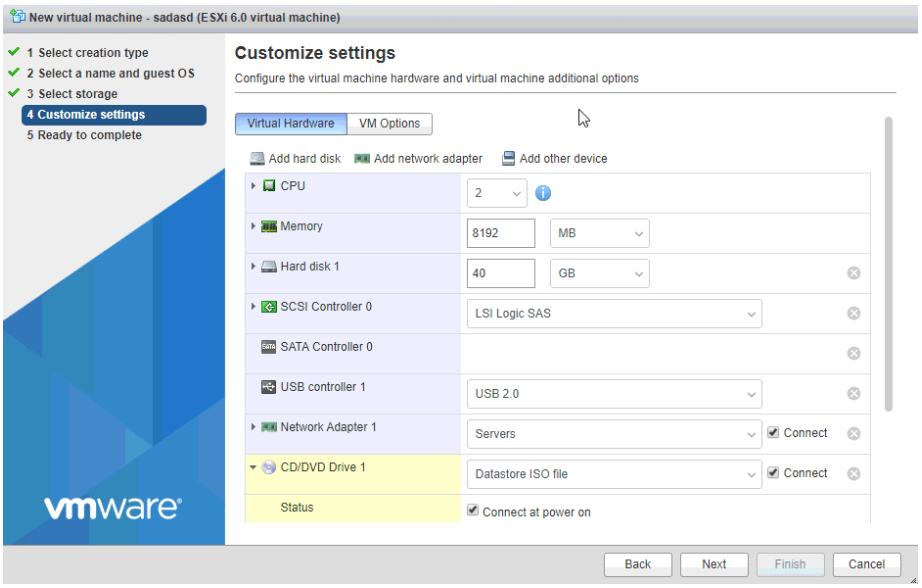
Obrázek 20 - VMware Vytváření dc1v č.2

Následně přiřadíme VM diskový prostor na řadiči, v našem případě zvolíme standartní přiřazení celého prostoru, který může být následně použit pro datové úložiště virtuálního serveru.



Obrázek 21 - VMware Vytváření dc1v č.3

Na další straně instalačního průvodce již zvolíme počet procesorových jader přiřazených pro tento stroj, velikost paměti RAM a velikost HDD (2 CPU jádra, 8192 MB RAM, 40 GB HDD). Taktéž zde můžeme zvolit síťový adaptér a instalační médium. Je nutné zakliknout kolonku pro připojení média, jinak nebude pro VM viditelné. Je zde vícero dalších možností, ale ty prozatím využívat nebudeme.

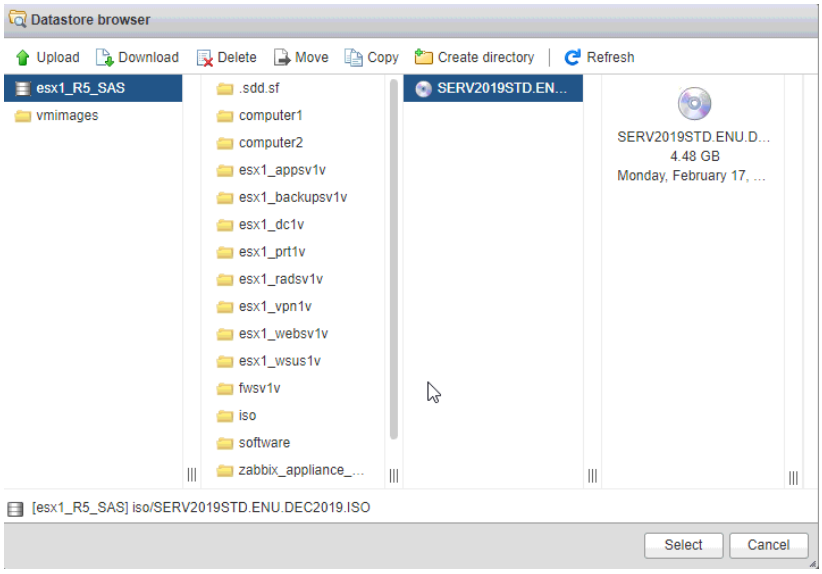


Obrázek 22 - VMware Vytváření dc1v č.4

Následuje už jen souhrn všech nastavení VM pro kontrolu a máme vytvořen první virtuální stroj. [14]

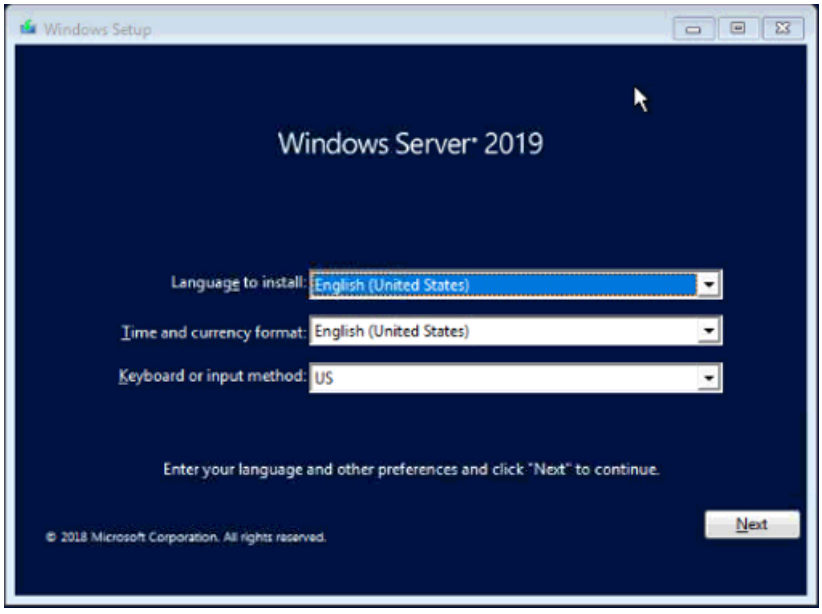
4.2.2 Instalace Windows Server 2019

Nyní jsme schopni nainstalovat server na náš nově vytvořený VM. Pro nahrání a zvolení instalačního média, které již máme vytvořené, je potřeba zvolit pravým tlačítkem myši náš vytvořený VM a pokračovat nabídkou Edit settings, kde pod kolonkou CD/DVD zvolíme Datastore ISO file, což nám nabídne pohled na data uložené na ESXi diskovém poli, vytvoříme si složku s libovolným názvem (pro nás „iso“). Poté zvolíme Upload a nahrajeme naše vytvořené instalační médium z počítače na hosta. Po dokončení nahrávání médium vybereme a dokončíme nastavení.



Obrázek 23 - Instalace Windows Server č.1

Spustíme Vm a otevřeme konzoli. Projdeme klasickou instalací Windows Serveru.

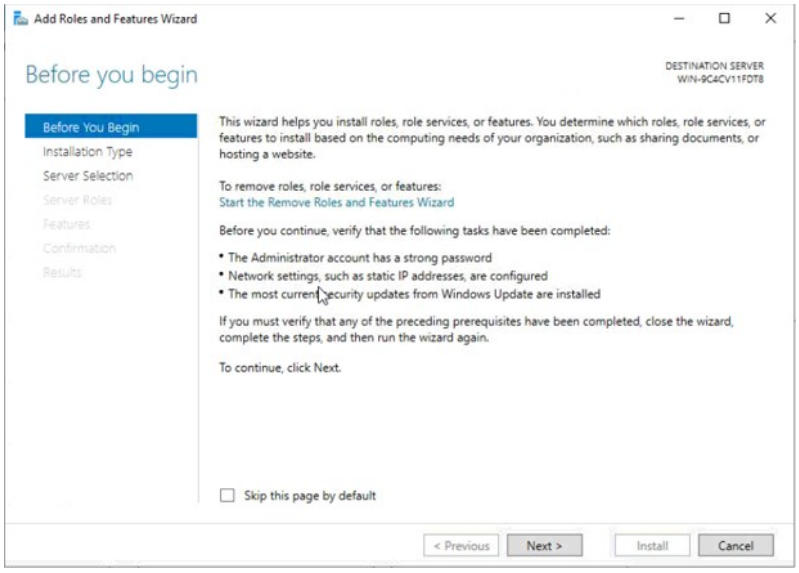


Obrázek 24 - Instalace Windows Server č.2

Po dokončení instalace zvolíme administrátorské heslo a systém provede prvotní konfiguraci. Velmi důležité je před započetím nainstalovat VMware tools, což je balíček ovladačů a konfiguračních souborů ulehčující práci s virtuálním strojem.

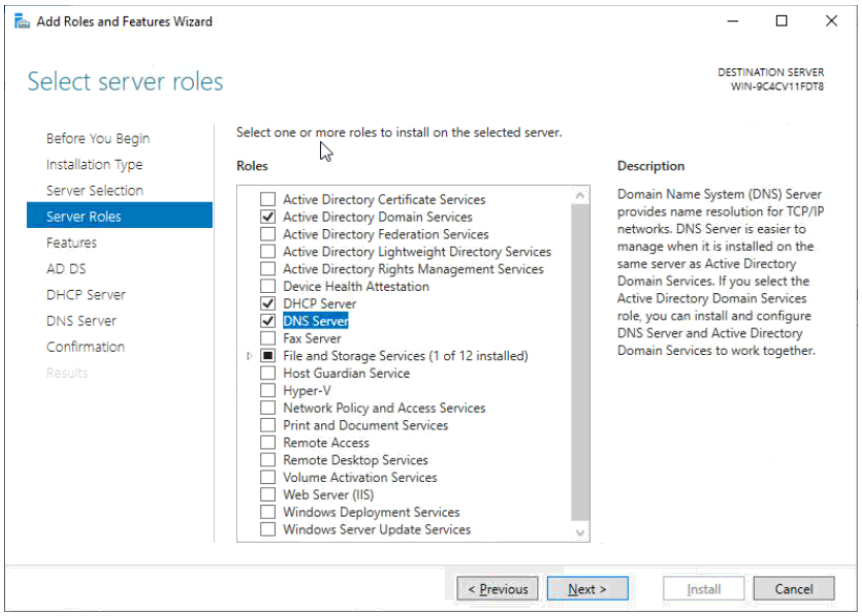
4.2.3 Instalace DC, ADDS, DNS a DHCP

Na tomto serveru zprovozníme služby Active Directory a zároveň budeme server konfigurovat jako doménový kontroler. Vzhledem k rozsahu síťové/serverové infrastruktury bude tento server zároveň poskytovat DHCP a DNS služby. Veškerá konfigurace serveru může probíhat z rozhraní Server manageru, které je uživatelsky přívětivá a poskytuje téměř vše, co budeme jako administrátor potřebovat. Pomocí Add roles and features přidáme serveru požadované funkce. [17]



Obrázek 25 - Konfigurace DC č.1

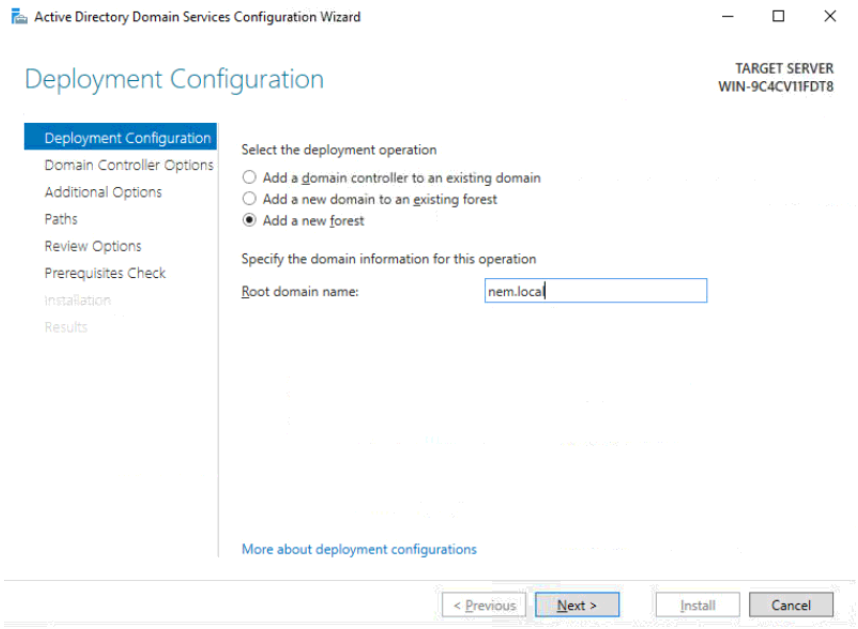
Na dalším listu zvolíme Role-based or feature based installation, následně zvolíme náš server (na který chceme služby přidat) a pokračujeme k výběru konkrétních služeb a funkcí. Zde vybereme již zmiňované ADDS, DHCP a DNS (u všech ještě vyskočí kontrolní okno s tlačítkem Add features). [17]



Obrázek 26 - Konfigurace DC č.2

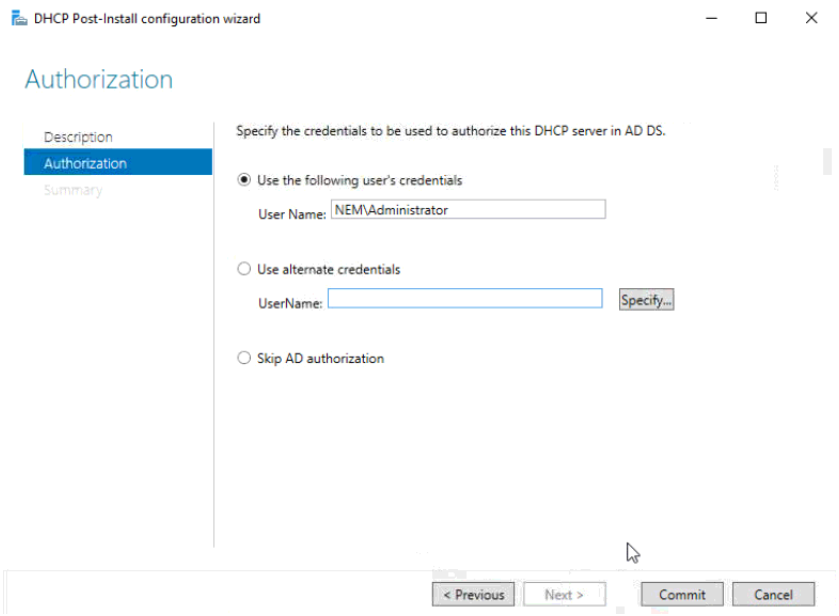
Dále pokračujeme v průvodci a započneme instalaci, po dokončení instalace vyzývá průvodce ke konfiguraci nových služeb. Je nutné povýšit náš server na doménový kontroler,

jinak nebude možné na něm využívat služeb ADDS a taktéž dokončit konfiguraci DHCP serveru. Prvně povýšíme server na DC, vytvoříme a pojmenujeme novou doménu. [17]



Obrázek 27 - Konfigurace DC č.3

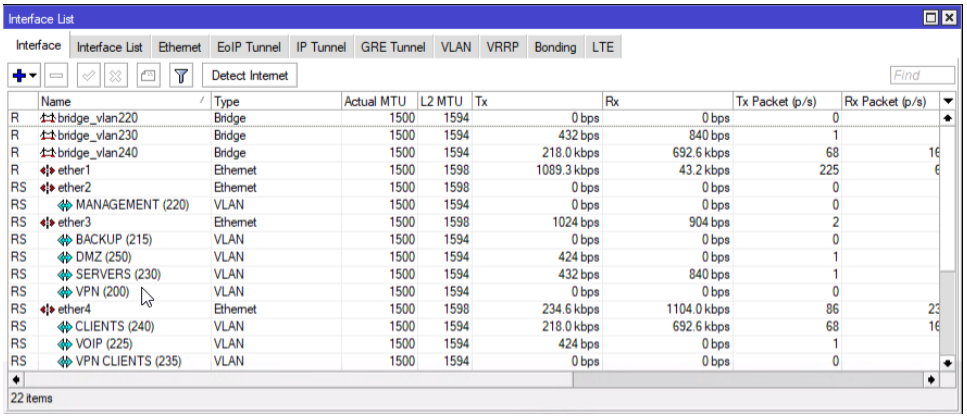
Dále zvolíme DSRM heslo (neboli heslo pro obnovu direktory services). Nebudeme vytvářet RODC (pouze pro čtení), neboť tohoto typu DC bychom využili například ve vzdálené lokalitě naší infrastruktury a toto DC by se poté odkazovalo pouze na primární DC. Poté již jen dokončíme instalaci. Server se následně sám restartuje, aby mohl zavést ADDS. Po restartu provedeme dodatečnou konfiguraci DHCP serveru, čímž jej připojíme k Active Directory, a tím samozřejmě i k doméně. [17]



Obrázek 28 - Konfigurace DC č.4

5 VYTVOŘENÍ OSTATNÍCH VLAN

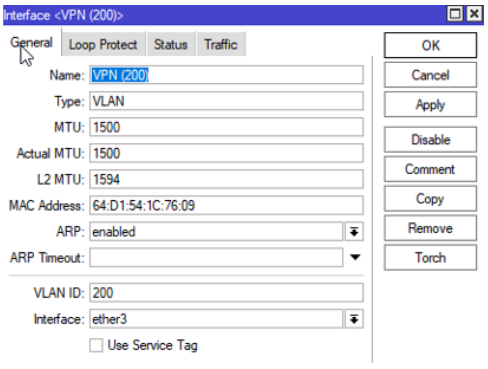
V jedné z předešlých kapitol jsme vytvořili první virtuální síť pro potřeby managementu ESXi. Nicméně naše infrastruktura ještě vyžaduje několikero dalších Vlan, abychom oddělili jednotlivé segmenty sítě a omezili tedy bezpečnostní nedostatky a ochránili servery a uživatele od zbytečných problémů. Budeme postupovat prakticky stejně jako při tvorbě první virtuální sítě, proto již nebude popsán postup, ale pouze zdokumentován. Je potřeba si Vlany pojmenovat a přiřadit jim rozdílná ID a pro všechny vytvořit adresní listy, díky čemuž se nám automaticky vygenerují směrovací trasy.



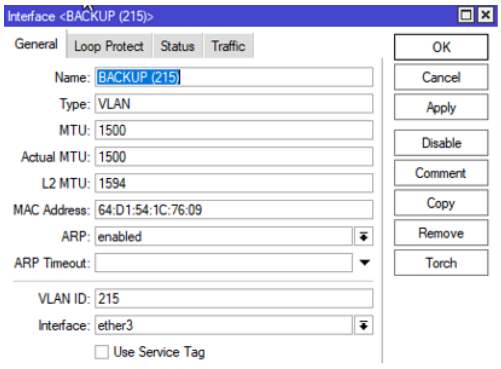
Obrázek 29 - Interface list

5.1 Konfigurace Vlan

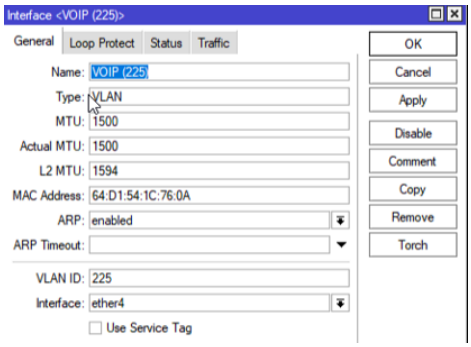
Nyní vytvoříme všechny požadované Vlany a přiřadíme je správným rozhraním. Prvně vytvoříme virtuální sítě pro rozhraní ether3 a poté pro ether4.



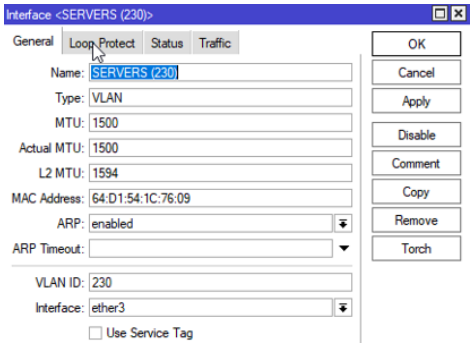
Obrázek 30 – VPN (200) Vlan



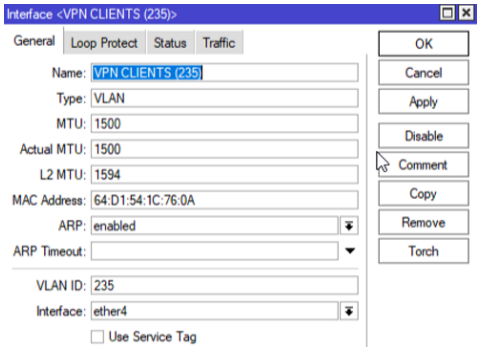
Obrázek 31 – Backup (215) Vlan



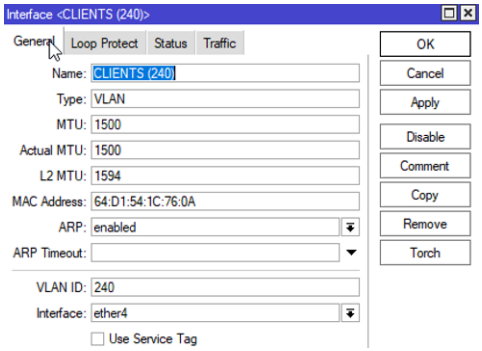
Obrázek 32 - VOIP (225) Vlan



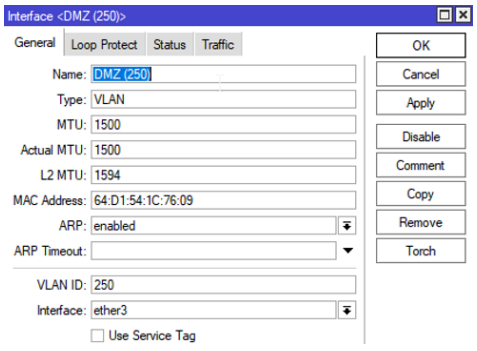
Obrázek 33 - Servers (230) Vlan



Obrázek 34 - VPN Clients (235) Vlan



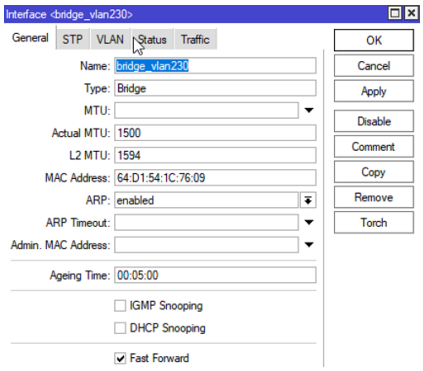
Obrázek 35 - Clients (240) Vlan



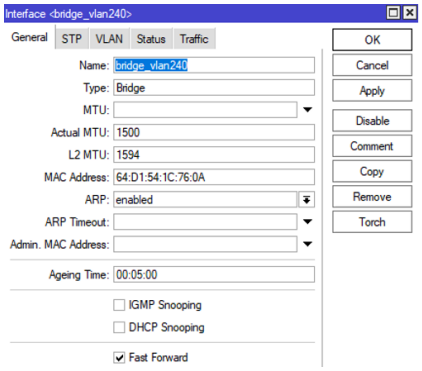
Obrázek 36 - DMZ (250) Vlan

5.1.1 Bridge a porty

Nejdříve vytvoříme nové bridge, a to bridge_vlan230 a bridge_vlan240.

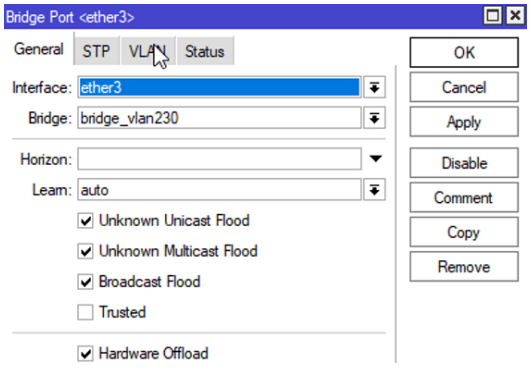


Obrázek 37 - Bridge_Vlan (230)

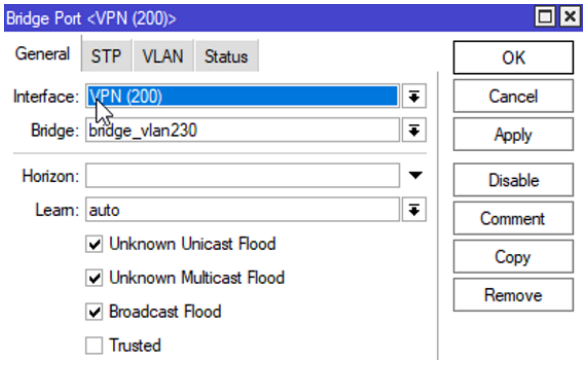


Obrázek 38 - Bridge_Vlan (240)

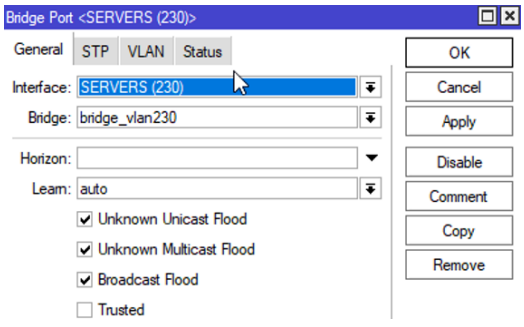
Následně vytvoříme porty, které přiřadíme k připraveným bridgům. Nejprve port pro ethernetový port č.3 následně porty pro VPN, Servery, DMZ a Backup, které přiřadíme k bridge_vlan230 a následně port pro ethernetový port č.4 a port pro Klienty, VOIP a VPN Klienty, které přiřadíme k bridge_vlan240.



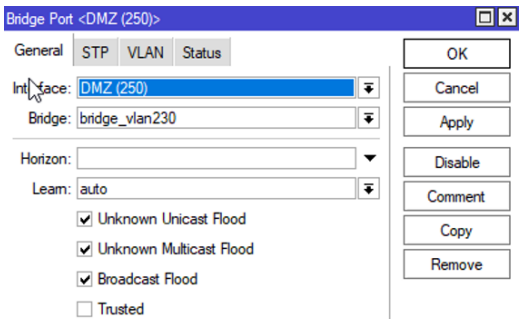
Obrázek 39 - Bridge_Vlan (230) port č.1



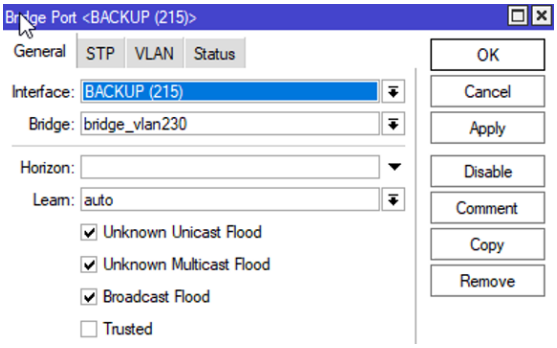
Obrázek 40 - Bridge_Vlan (230) port č.2



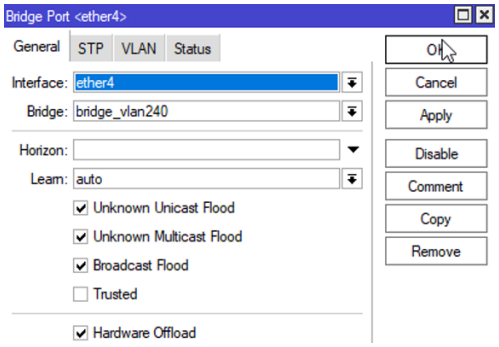
Obrázek 41 - Bridge_Vlan (230) port č.3



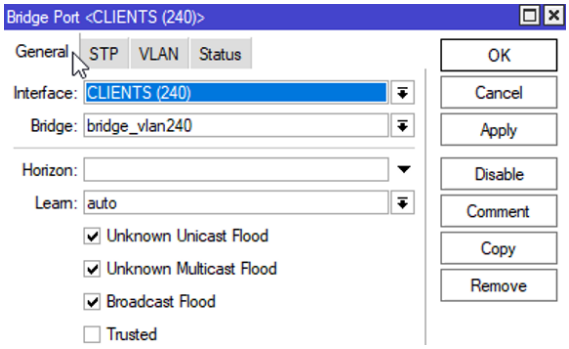
Obrázek 42 - Bridge_Vlan (230) port č.4



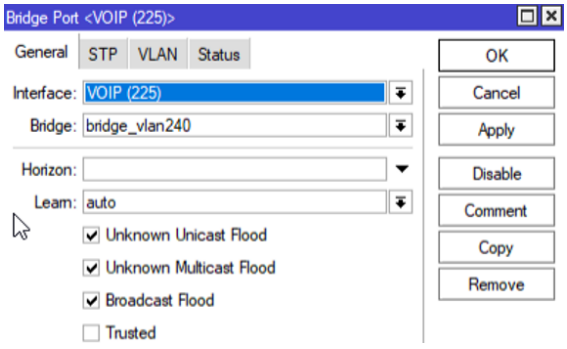
Obrázek 43 - Bridge_Vlan (230) port č.5



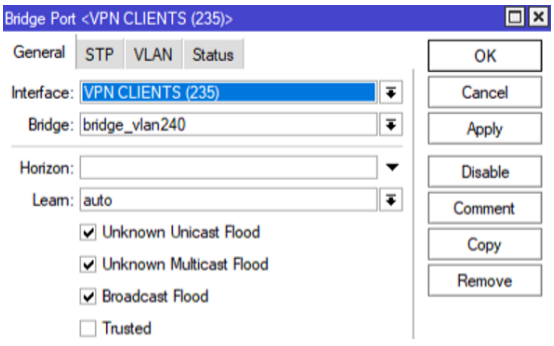
Obrázek 44 - Bridge_Vlan (240) port č.1



Obrázek 45 - Bridge_Vlan (240) port č.2



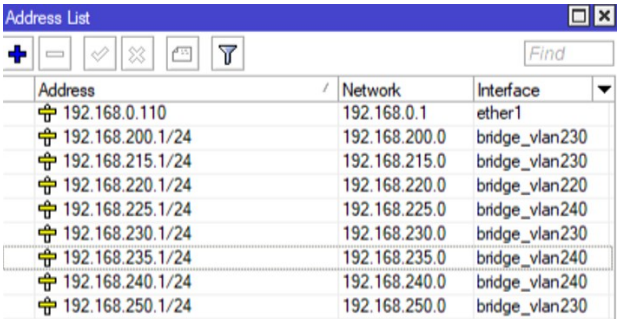
Obrázek 46 - Bridge_Vlan (240) port č.3



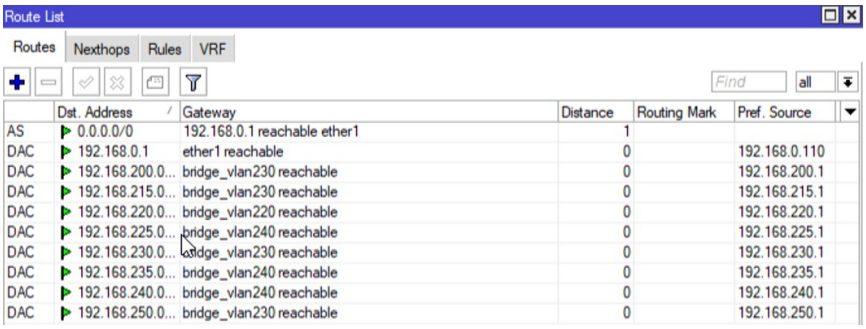
Obrázek 47 - Bridge_Vlan (240) port č.4

5.1.2 Adresní pole

Nyní pro každou Vlanu musíme vytvořit adresní list, abychom byli schopni přiřadit určitou adresu právě k této virtuální síti, a naopak odlišit adresy z jiných sítí.



Obrázek 48 - Address List

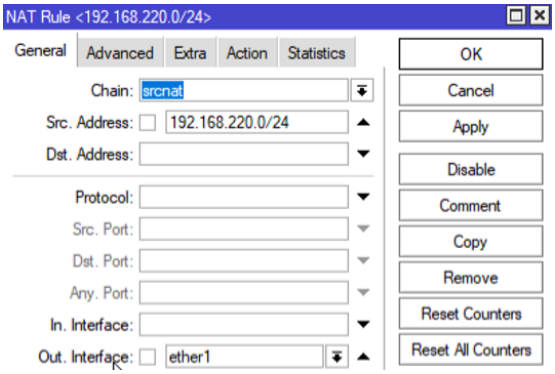


Obrázek 49 - Route List

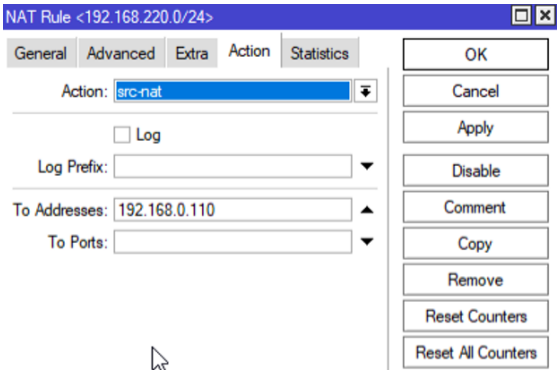
5.1.3 Firewall NAT

Pro správnou funkčnost VLAN ještě musíme pro každou Vlanu vytvořit pravidlo, aby byl L3 switch schopný směrovat správně síťový tok.

Zvolíme IP/Firewall, kde následně vybereme kolonku NAT. Nyní již nebudeme potřebovat naše vytvořené pravidlo a vytvoříme pravidla pro každou VLANu odděleně, aby bylo možné na jednotlivých pravidlech kontrolovat provoz. V části general zvolíme srcnat a Src. Address: 192.168.220.0/24, dále pak zvolíme odchozí interface Out. Interface: ether1. V liště Action pak zvolíme Action: src-nat a zadáme adresu našeho L3 switche do To Addresses: 192.168.0.110.

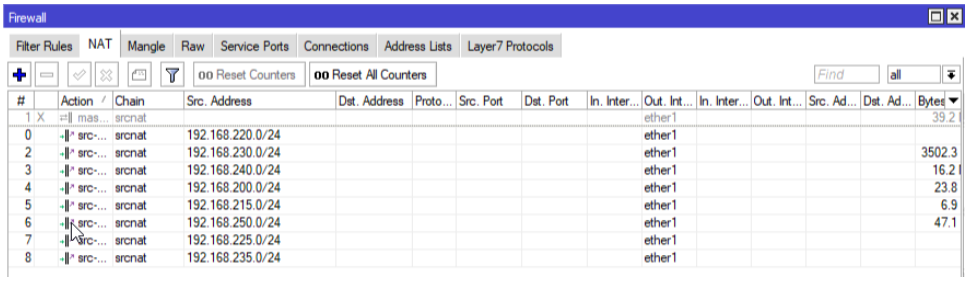


Obrázek 50- NAT rule (220) č.1



Obrázek 51 - NAT rule (220) č.2

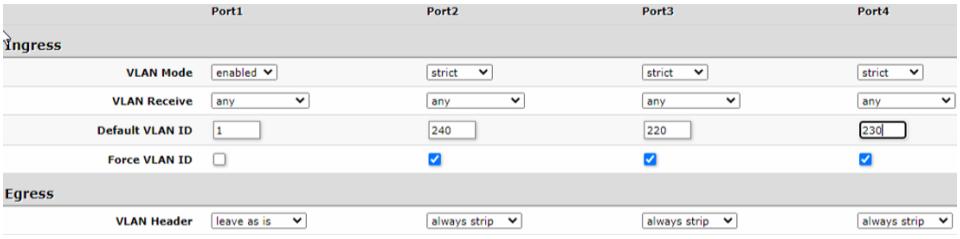
Všechny ostatní pravidla vytvoříme stejným způsobem se správnými atributy. Kdy po vytvoření všech pravidel následně pomocí křížku zakážeme naše původní pravidlo. [15]



Obrázek 52 - NAT

6 ZAPOJENÍ FYZICKÉHO SWITCHE

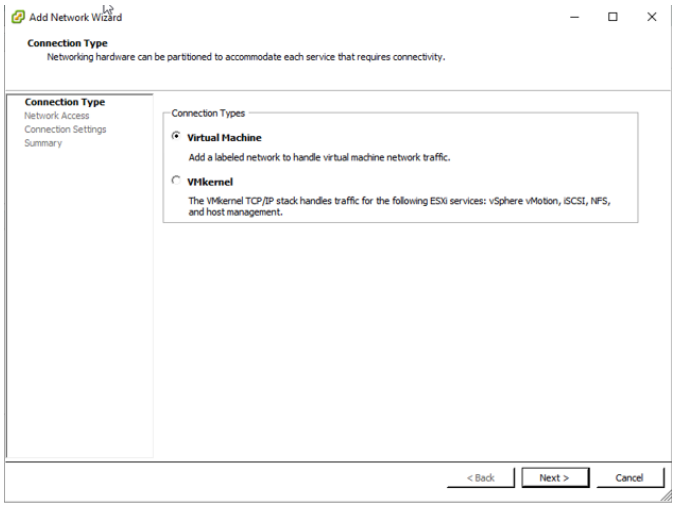
Vzhledem k obecné praxi, kde většinově se v menších i větších společnostech počítá s větším množstvím klientů, zavedeme i v našem případě použití L2 switche jako síťový prvek mezi naším L3 switchem (který využívám taktéž jako router) a virtuálními switchi na ESXi. Bude nám simulovat připojení klientských počítačů (které nám bude poskytovat samotný ESXi host) a klasické zapojení do fyzického switche v rámci naší fiktivní společnosti. Nebudeme tudíž zapojovat přímo virtuální switch do našeho L3 Mikrotiku, nýbrž bude virtuální uživatelský počítač zapojen do fyzického Mikrotik switche, který bude dělat prostředníka mezi ESXi a L3 switchem. Stejným způsobem budou propojeny i ostatní subnety, abychom nasimulovali reálné zapojení v praxi. Zároveň bude do tohoto switche zapojen napřímo i počítač, odkud budeme provádět penetrační testování. Pro správnou funkčnost nastavíme switch pro funkčnost v rámci Vlan sítí a posléze můžeme zapojit ethernetové kabely. [15]



Obrázek 53 – Mikrotik switch konfigurace

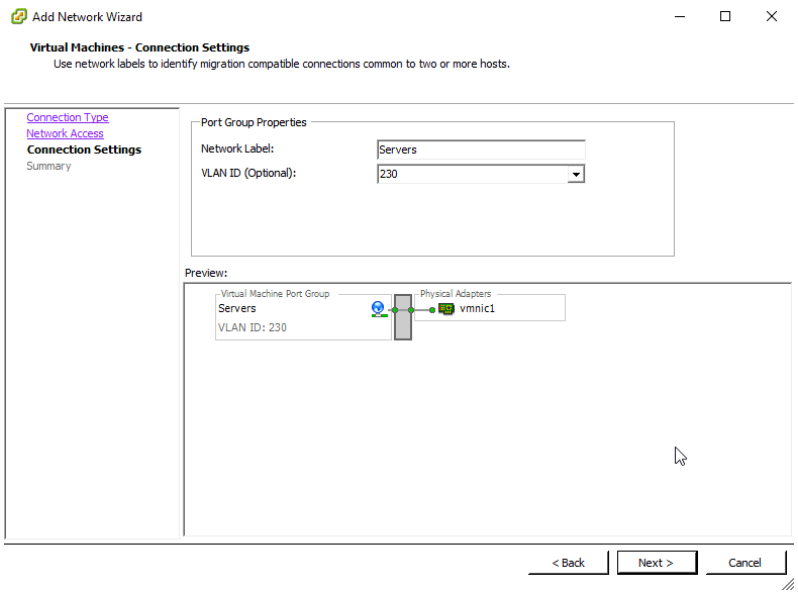
7 VYTVOŘENÍ VIRTUÁLNÍHO SWITCHE

Nyní, když máme vytvořené jednotlivé virtuální sítě, využijeme možností VMware a pomocí Vsphere vytvoříme virtuální switch, který bude posílat pakety s konkrétním id na korektní zařízení na ESXi. Ve firmě tento post zastává další fyzický switch, který byl taktéž otestován pro kontrolní účely, nicméně nadále využíváme pouze služeb Vsphere. Jak již bylo zmíněno, pro konfiguraci virtuálního switch využijeme možností lokálního klienta Vsphere, neboť poskytuje lepší vizuální zobrazení a je pro tento úkon přehlednější. V menu zvolíme Configuration/Networking, poté Add networking v novém okně následně vybereme Virtual Machine. [14]



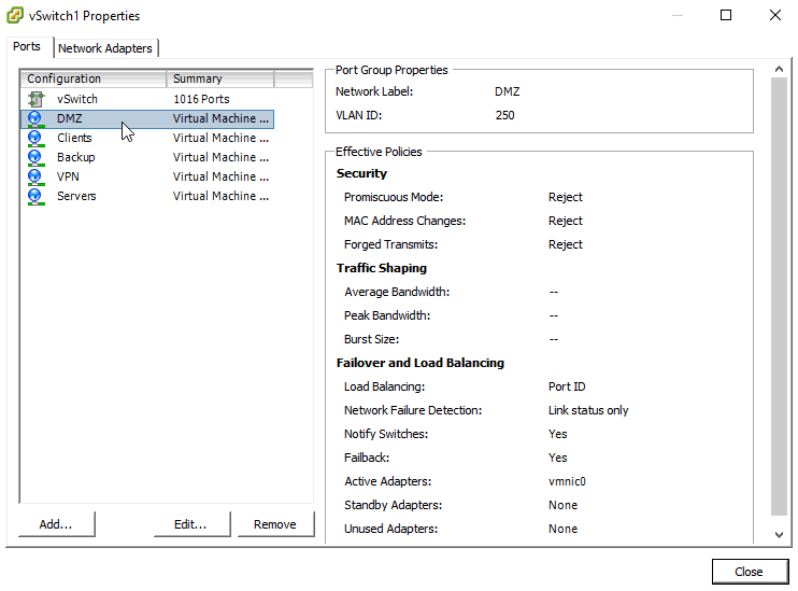
Obrázek 54 - Tvorba virtuálního switche č.1

V následujícím okně vybereme, přes kterou fyzickou síťovou kartu poputuje síťový provoz. Pro každý virtuální switch by měly být ideálně zvoleny dvě, aby při výpadku jedné karty bylo možné ethernetový kabel jen přepojit do druhého portu. Zvolíme požadovaný název a přiřadíme id dle id Vlany, která bude k tomuto portu připojen.



Obrázek 55 - Tvorba virtuálního switche č.2

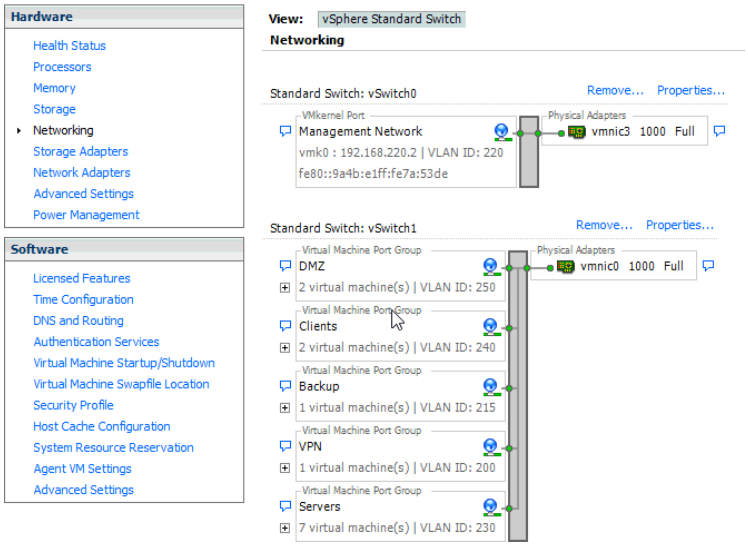
Neboť využíváme trunkového připojení, budeme jedním portem přenášet vícero Vlan s různými ID, a proto vytvoříme další potřebné skupiny portů. Zvolíme properties u našeho nového switche, kde vytvoříme skupiny pro DMZ, Clients, Backup a VPN.



Obrázek 56 - Tvorba virtuálního switche č.3

Vzhledem k obecné praxi, kdy management síť, jak již bylo zmíněno, má být úplně oddělena od ostatních sítí, tak získáme konfiguraci virtuálních switchů takovou, že první ze dvou switchů bude předávat pouze Vlan ID 220 a tudíž funguje pouze jako management switch a

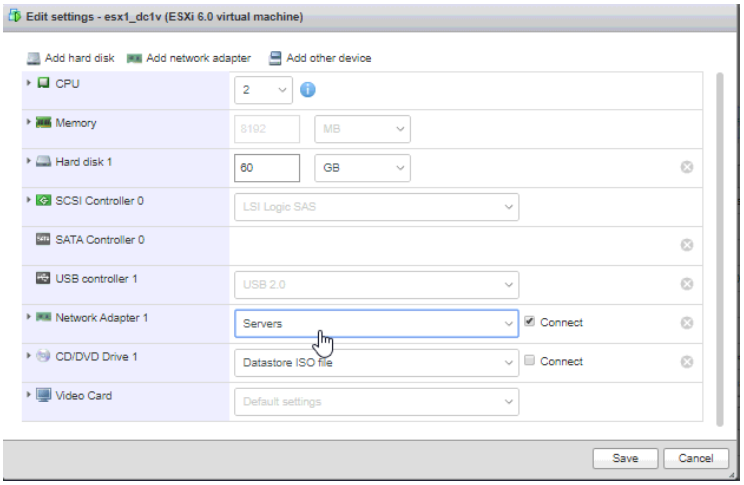
má jen jednu port skupinu, kdežto druhý předává ID všech ostatních sítí a má proto vícero port skupin.



Obrázek 57 - Tvorba virtuálního switche č.4

7.1 Přiřazení DC do port skupiny

Musíme ještě provést změnu na našem VM, zvolíme proto „Edit settings“, kde vybereme nový Network adapter a zvolíme již vytvořené Servers, čímž VM přiřadíme do port skupiny s ID 230.

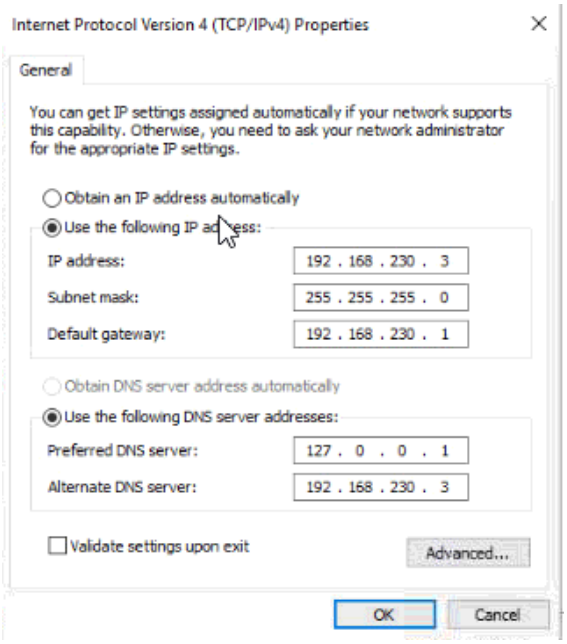


Obrázek 58 - Přiřazení VM do skupiny portů

8 PŘIŘAZENÍ IP ADRESY DC A KONFIGURACE DNS A DHCP

8.1 Přiřazení statické IP adresy doménovému kontroleru

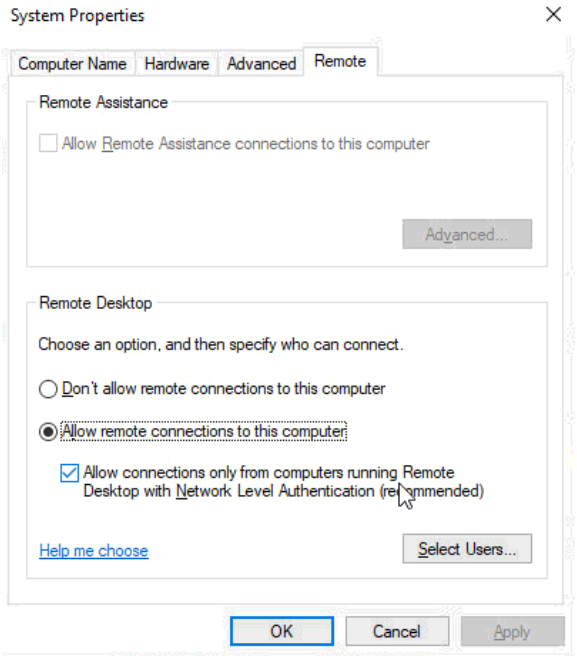
Nyní jsme schopni našemu serveru přiřadit funkční statickou adresu. Dále nastavíme nový rozsah, který bude poskytovat DHCP server klientům. Všechny servery budou mít statickou IP adresu, a tudíž je zbytečné pro ně vytvářet dynamický rozsah. Zvolíme statickou IP adresu 192.168.230.3, dále bránu 192.168.230.1 a poté náš již vytvořený DNS server, který má primárně lokální adresu 127.0.0.1, protože se nachází na stejném serveru a sekundární adresa je 192.168.230.3 virtuálního serveru.



Obrázek 59 - DC Síťový Adaptér

8.2 Povolení RDP

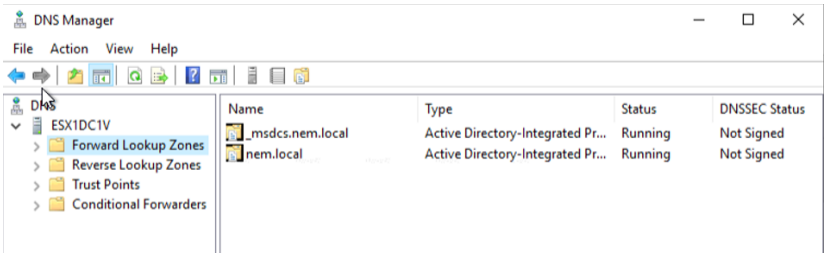
Pro lepší práci s virtuálním serverem povolíme RDP (Remote desktop protocol) připojení. Pomocí nabídky properties (vlastnosti) při pravém tlačítku na This pc (Tento počítač) otevřeme nové okno, kde zvolíme Advanced systém settings (Upřesnit nastavení systému), rozevřeme lištu Remote (vzdálený přístup), kde povolíme již zmiňovaný RDP.



Obrázek 60 - DC povolení RDP

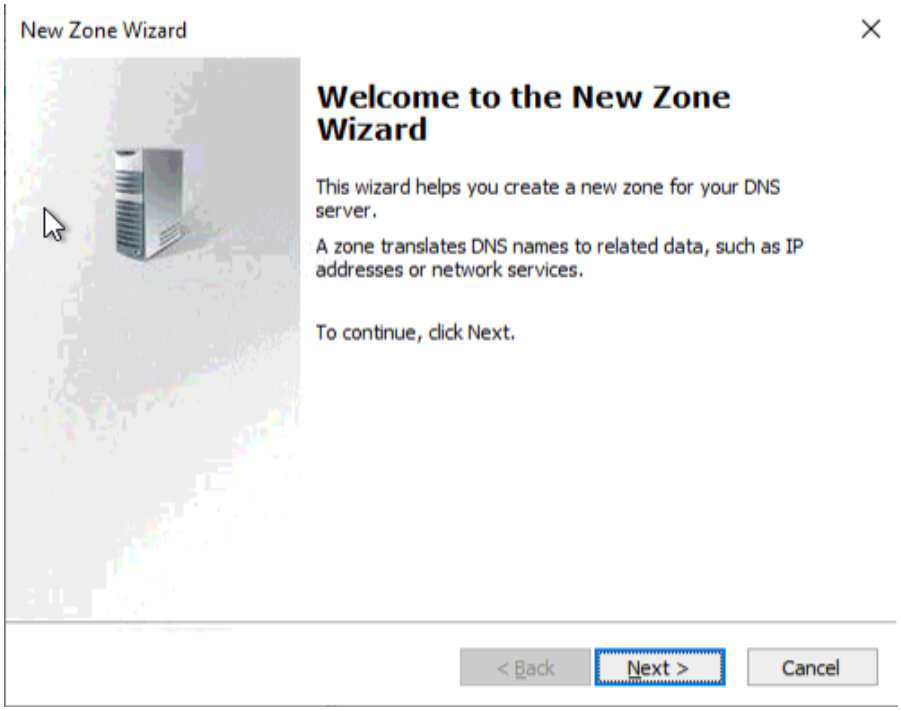
8.3 Nastavení DNS serveru

Pro nastavení DNS serveru použijeme DNS manager, kde již máme vygenerovanou zónu nem.local, kterou jsme vytvořili při instalaci DNS a taktéž _msdcs.nem.local, která je rezervována pro Microsoft a proto uživatel například při žádosti na LDAP (DC) server ví, že bude kontaktován Microsoft doménový kontroler. A totéž platí pro ostatní Microsoft služby.



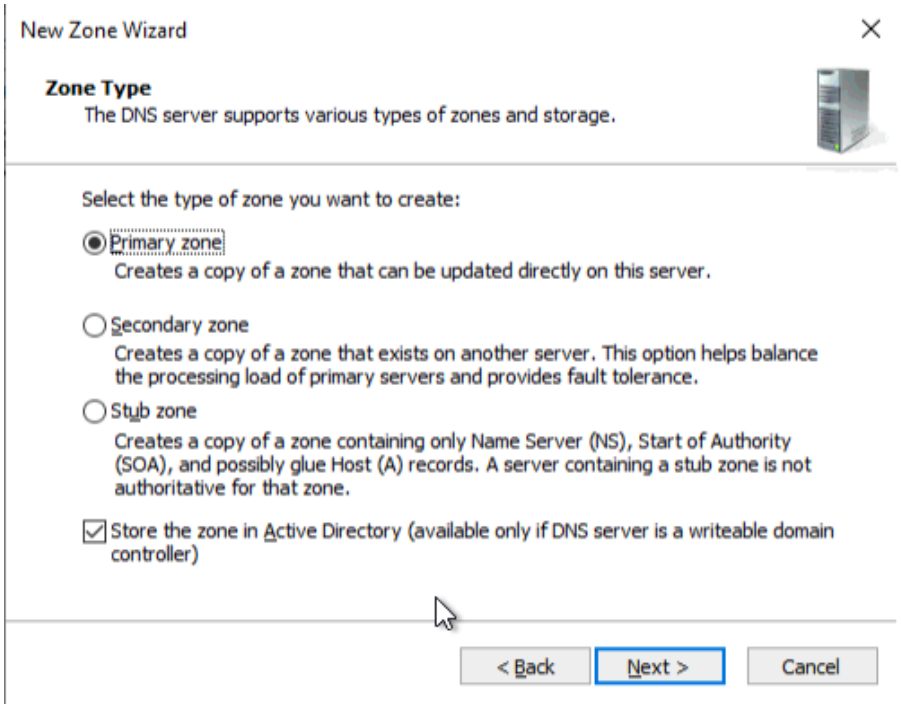
Obrázek 61 - DNS konfigurace

Nyní již DNS server umí vyhledávat v doménovém stromu, nyní však je ještě potřeba vytvořit zóny pro zpětný překlad jmen.

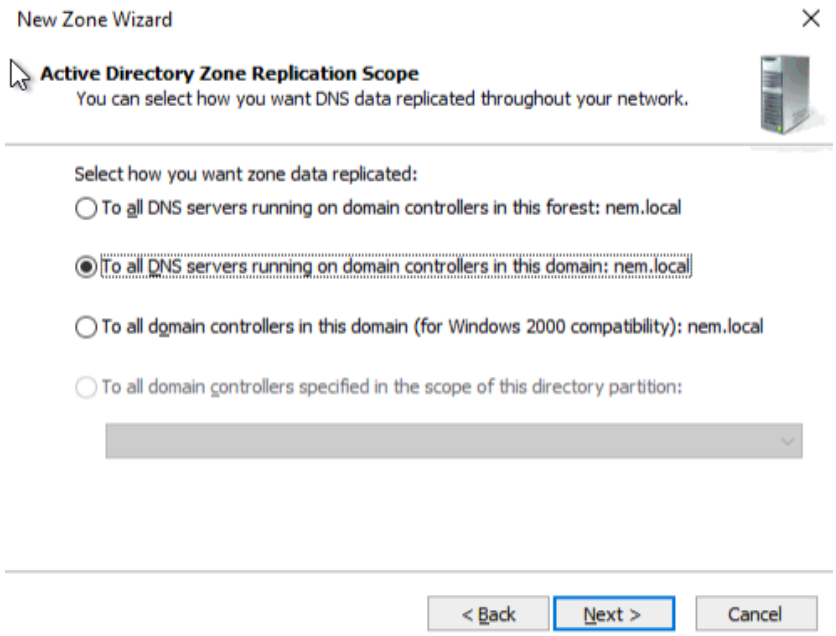


Obrázek 62 - DNS konfigurace č.2

V části Reverse Lookup Zones pravým tlačítkem vytvoříme novou primární zónu dostupnou pro všechny DC kontrolery.

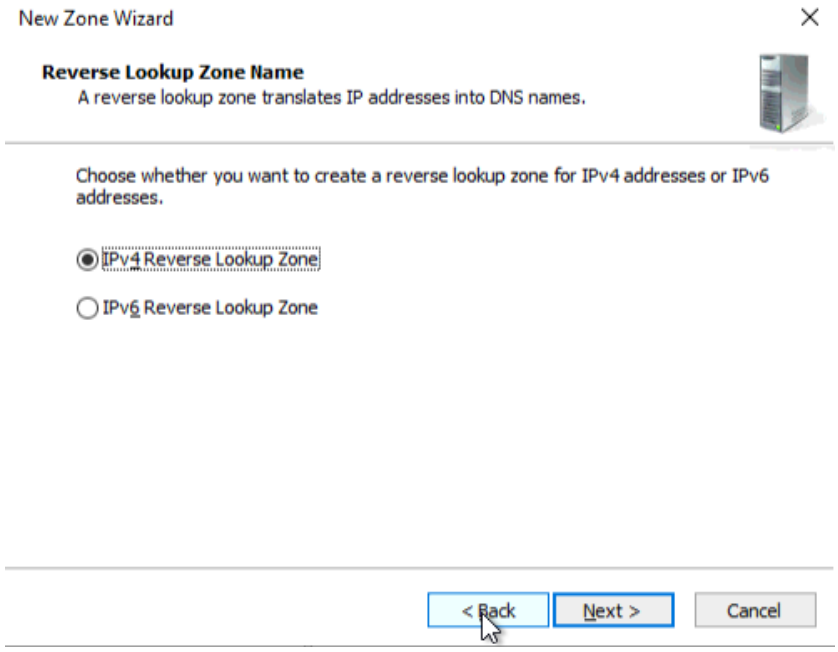


Obrázek 63 - DNS konfigurace č.3

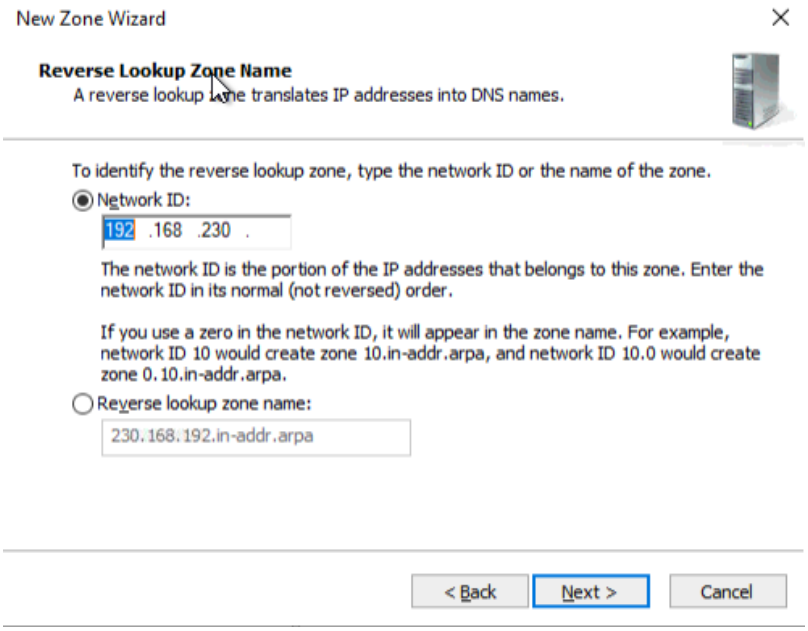


Obrázek 64 - DNS konfigurace č.3

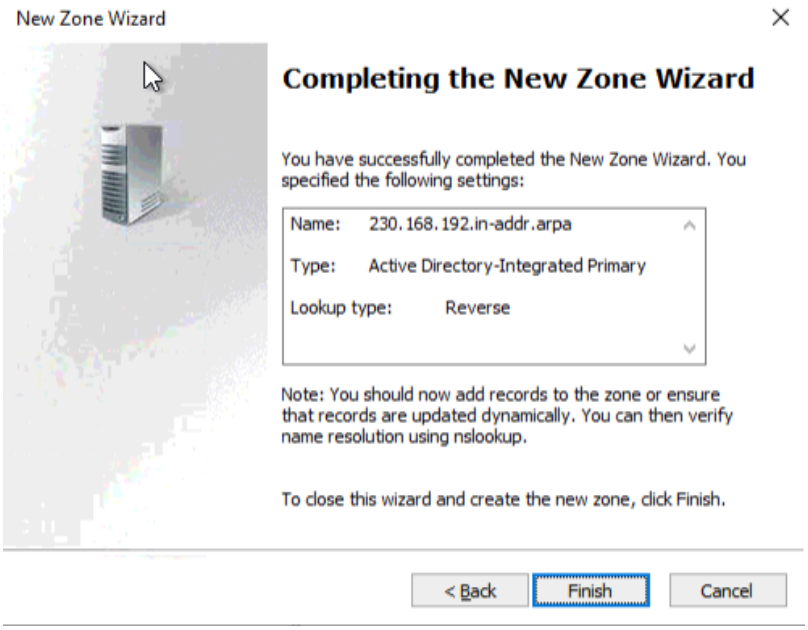
V našem případě je pouze jeden, zvolíme IPv4 a následně zadáme náš adresní rozsah 192.168.230, dále zvolíme pouze zabezpečené dynamické aktualizace, což je doporučeno pro AD. [17]



Obrázek 65 - DNS konfigurace č.4

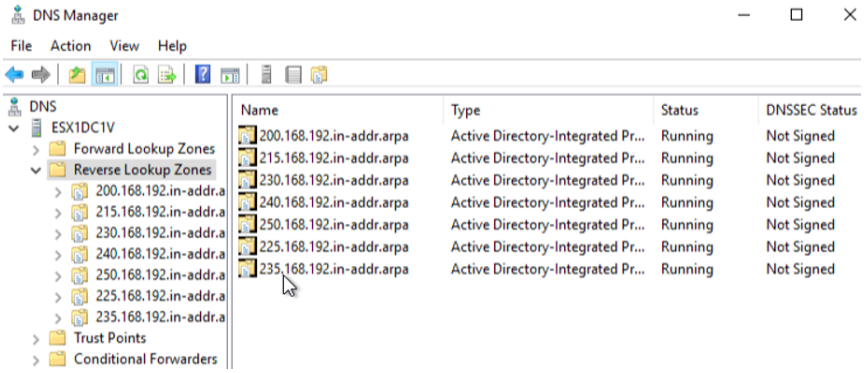


Obrázek 66 - DNS konfigurace č.5



Obrázek 67 - DNS konfigurace č.6

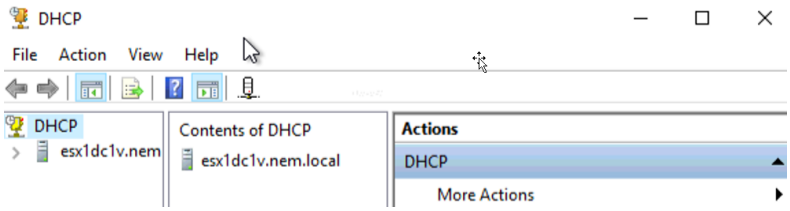
Následně tímto postupem vytvoříme reverzní zóny pro všechny naše již vytvořené VLANy, neboli subnety, abychom při přidání serverů a zařízení již nemuseli k tomuto vracet a DNS server si samostatně necháme vytvořit pouze forward zóny a následně pointery pro jednotlivé klienty/servery.



Obrázek 68 - DNS konfigurace č.7

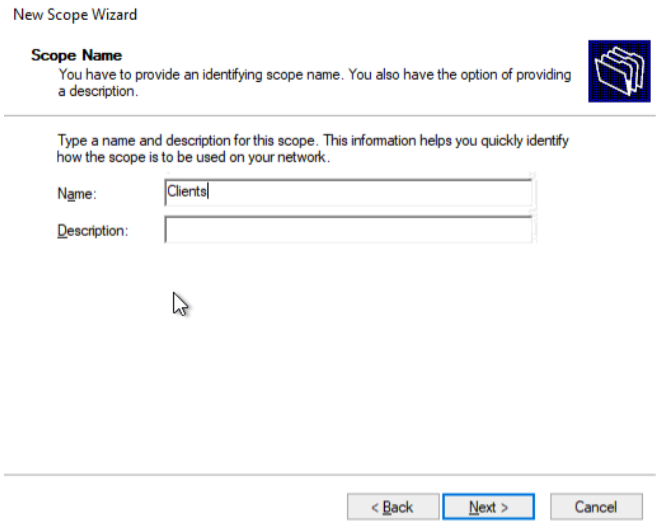
8.4 Konfigurace DHCP

Konfiguraci DHCP budeme provádět v DHCP manageru, kde vzhledem k potřebám zadání vytvoříme pouze 3 dynamicky alokovaná adresní pole, neboť servery, jak již bylo zmíněno, budou mít statické adresy a není tedy nutné, aby v jejich VLANech byly dynamicky přiřazované adresy. Tudíž vytvoříme dynamicky distribuované pole adres pro klienty, což jsou notebooky a počítače, následně druhé pole pro VOIP linky, a nakonec třetí pole pro klienty VPN připojení.



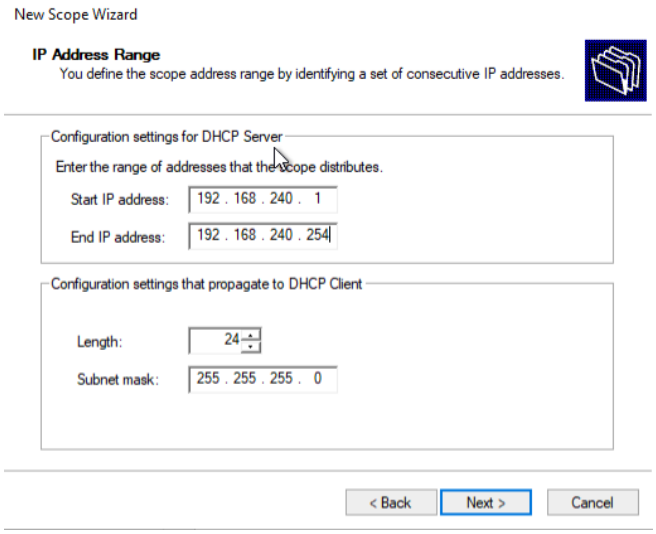
Obrázek 69 - DHCP konfigurace

Vybereme náš DHCP server esx1dc1v.nem.local, dále pak pravým tlačítkem na IPv4, kde vybereme New scope. Následně jej pojmenujeme, popíšeme a dále zvolíme adresní rozsah, který tvoří scope, ze kterého server poskytuje IP adresy (pro Clients je rozsah 192.168.240.1-192.168.240.254).

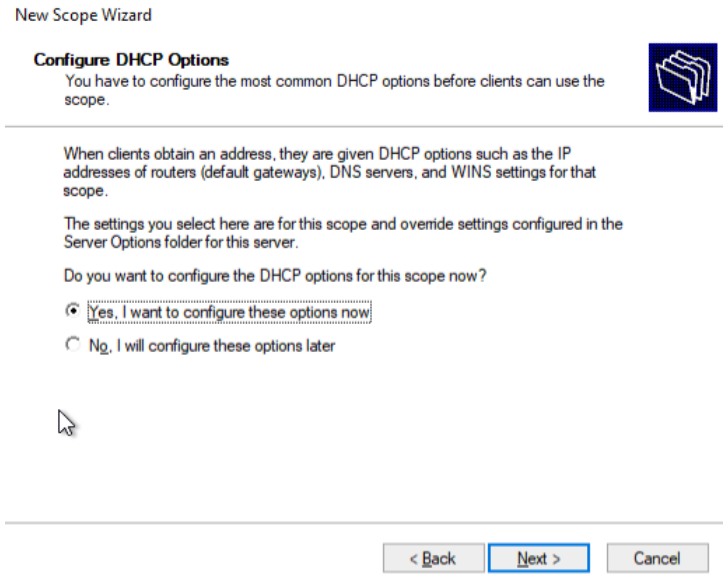


Obrázek 70 - DHCP konfigurace č.2

Stejným způsobem pak vytvoříme dynamické rozsahy pro ostatní VOIP a VLAN CLIENTS. [17]

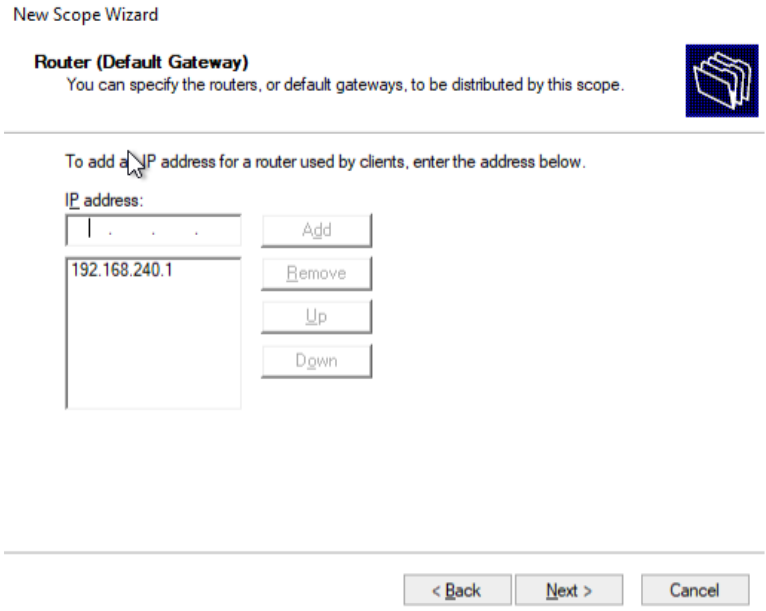


Obrázek 71 - DHCP konfigurace č.3

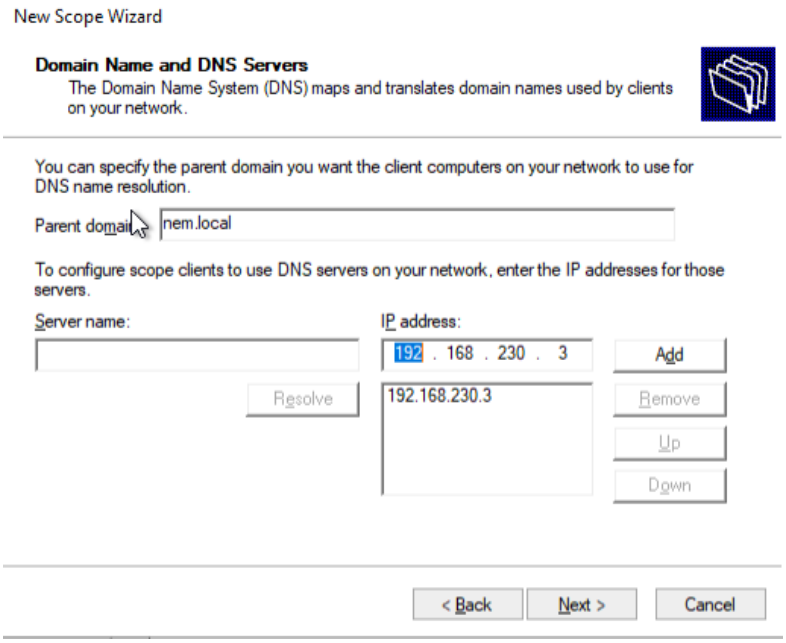


Obrázek 72 - DHCP konfigurace č.4

Pak již jen zvolíme výjimky a délku rezervace adresy pro jednoho žadatele. Dále potvrdíme okamžitou platnost našich nastavení a přidáme bránu či router pro náš subnet, kterou bude DHCP server taktéž distribuovat. Pokračujeme zadáním naší domény nem.local a IP adresy DNS serveru (192.168.230.3) a pak již jen dokončíme.



Obrázek 73 - DHCP konfigurace č.5



Obrázek 74 - DHCP konfigurace č.6

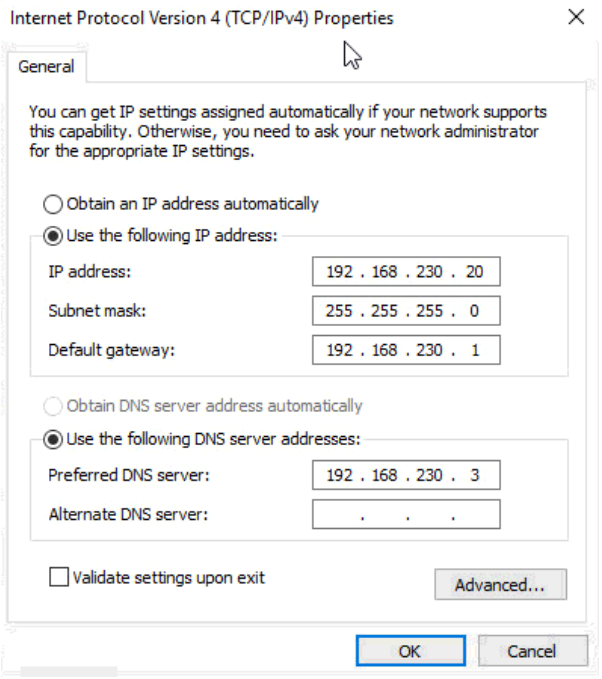
9 VYTVOŘENÍ A KONFIGURACE FILESERVERU

9.1 Vytvoření VM

Prvotně založíme nový virtuální stroj pomocí Vsphere nebo webového rozhraní (viz podkapitoly 4.2.1 a 4.2.2), kde jako název VM bude esx1_fs1v a název serveru fs1v a přiřadíme do virtuální síťové skupiny Servers (viz kapitola 6.1). Serveru přiřadíme 1 jádro a 2048Mb RAM. Po dokončení instalace Windows začneme s konfigurací síťové karty.

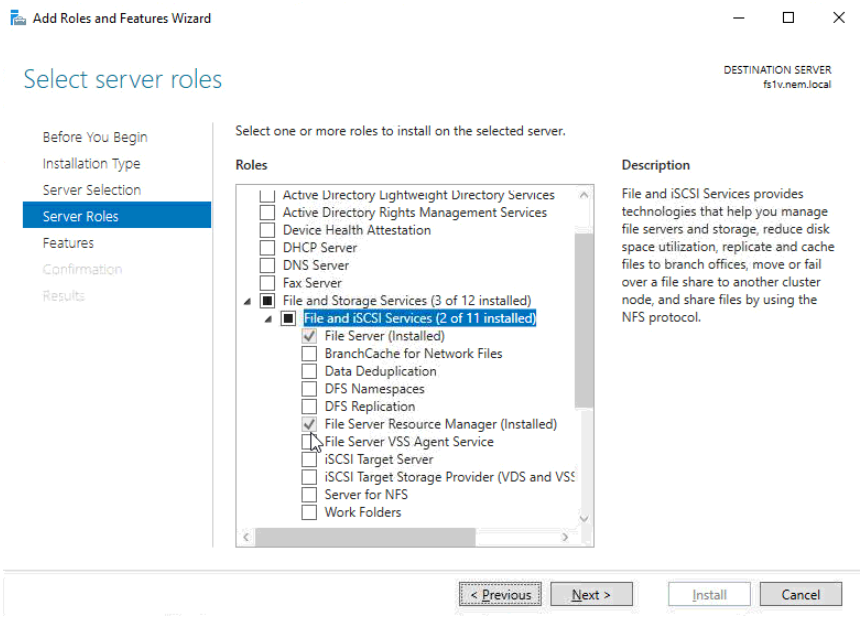
9.2 Konfigurace serveru

Prvně přiřadíme statickou IP adresu 192.168.230.20 stejně jako v případě DC (viz kapitola 7.1). Nyní již použijeme náš DNS server.



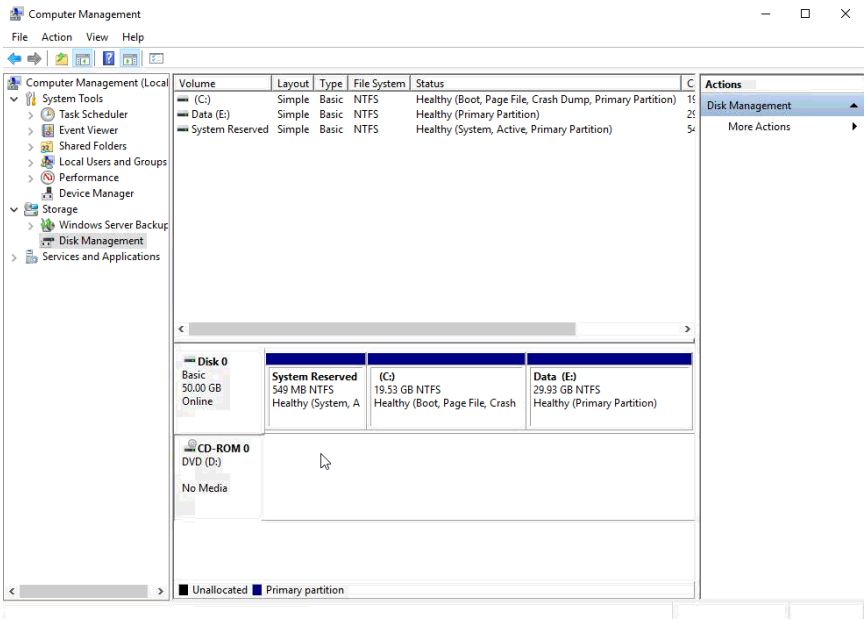
Obrázek 75 - Fileserver síťový adaptér

Dále budeme postupovat stejně jako u serveru DC. Nastavíme jméno, přiřadíme do domény, povolíme vzdálený přístup a poté se pustíme do samotné instalace funkcí fileserveru. Pomocí Server Manageru přidáme „File Server Resource Manager“ a dokončíme instalaci, která nevyžaduje restart celého serveru.

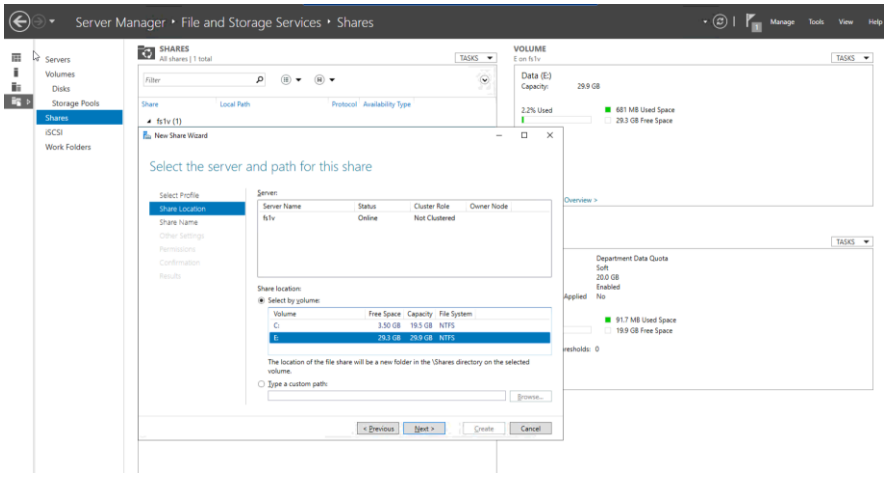


Obrázek 76 - Fileserver konfigurace

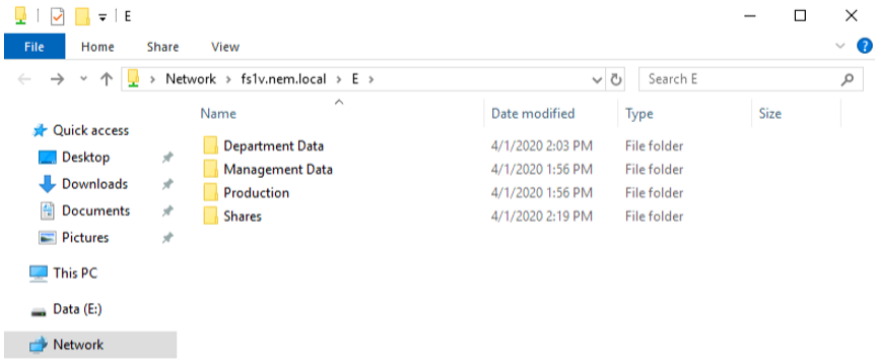
Pomocí Správy počítače rozdělíme disk serveru na 2 oddíly (systémový a datový), abychom oddělili uživatelská data od serveru samotného. Následně pomocí Server Manageru vytvoříme share na celý oddíl. V nově vytvořeném a sdíleném oddíle si vytvoříme požadované složky.



Obrázek 77 - Fileserver konfigurace č.2



Obrázek 78 - Fileserver konfigurace č.3

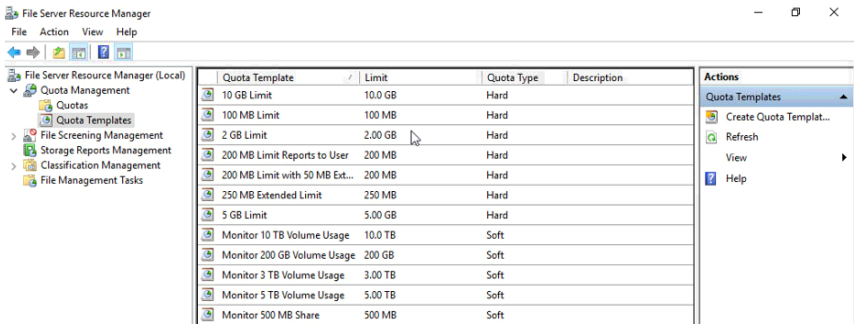


Obrázek 79 - Fileserver konfigurace č.4

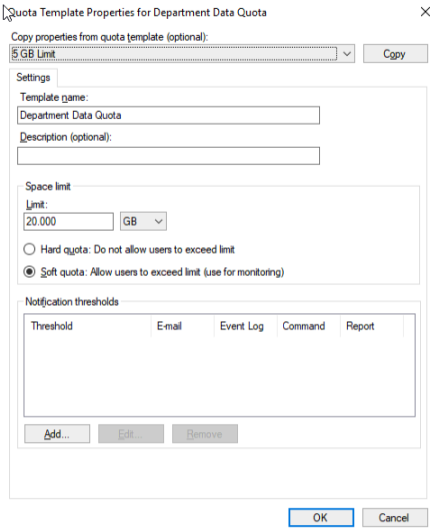
V rámci nastavení Resource manageru se budeme zajímat o definování kvóty a restrikce typů ukládaných souborů.

9.2.1 Definování kvóty

kde si kromě možnosti výběru předdefinovaných šablon, vytvoříme kvótu novou, pomocí založení nové šablony Create Quota Template. Kde vybereme vzor 5GB, datovou kapacitu kvóty 20GB, zda se jedná o Hard, či Soft kvótu, kde u první nelze přesáhnout kapacita, kdežto u druhé možnosti kapacita může být přesažena a slouží spíše k monitoringu. Volíme druhou možnost. [17]



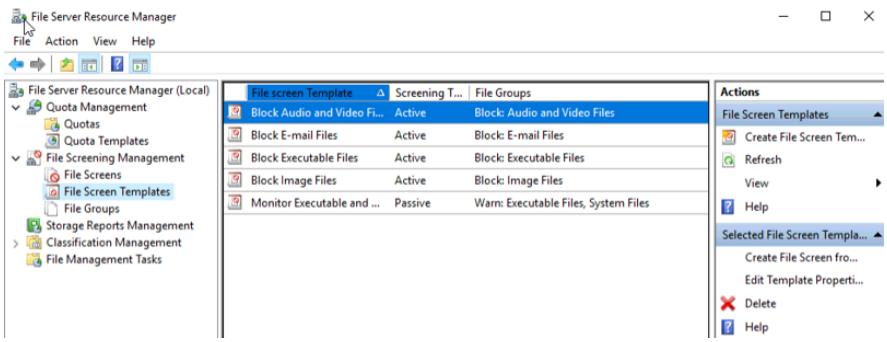
Obrázek 80 - Fileserver konfigurace č.5



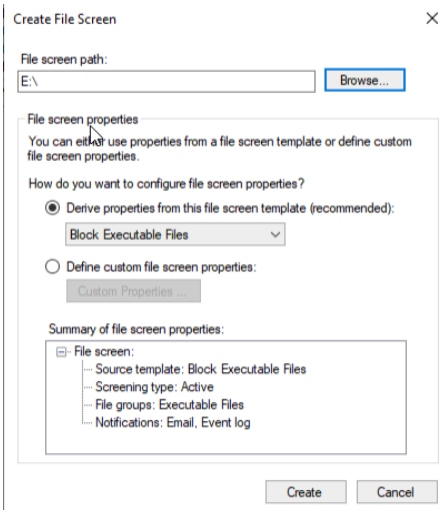
Obrázek 81 - Fileserver konfigurace č.6

9.2.2 Definice povolených souborových typů

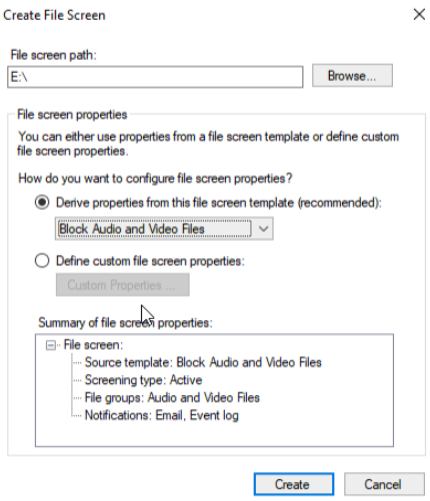
V části „File Screening“ vybereme žádané šablony. Je samozřejmě možné si vytvořit vlastní, nicméně my využijeme již nachystané. Zvolíme Block Audio and Video Files a následně pravým klikem vytvoříme nové pravidlo, vybereme cestu na náš share (E:) a dokončíme. Stejný proces ještě provedeme ještě se šablonou pro blokaci spustitelných souborů. [17]



Obrázek 82 - Fileserver konfigurace č.7



Obrázek 83 - Fileserver konfigurace č.8

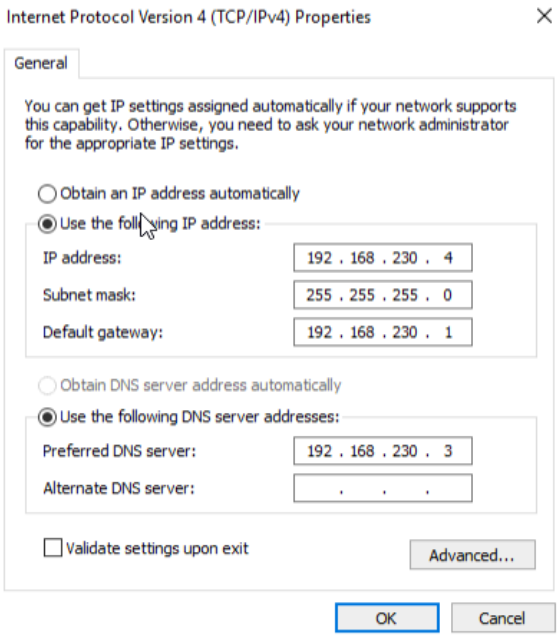


Obrázek 84 - Fileserver konfigurace č.9

10 VYTVOŘENÍ A KONFIGURACE PRINTSERVERU

10.1 Konfigurace serveru

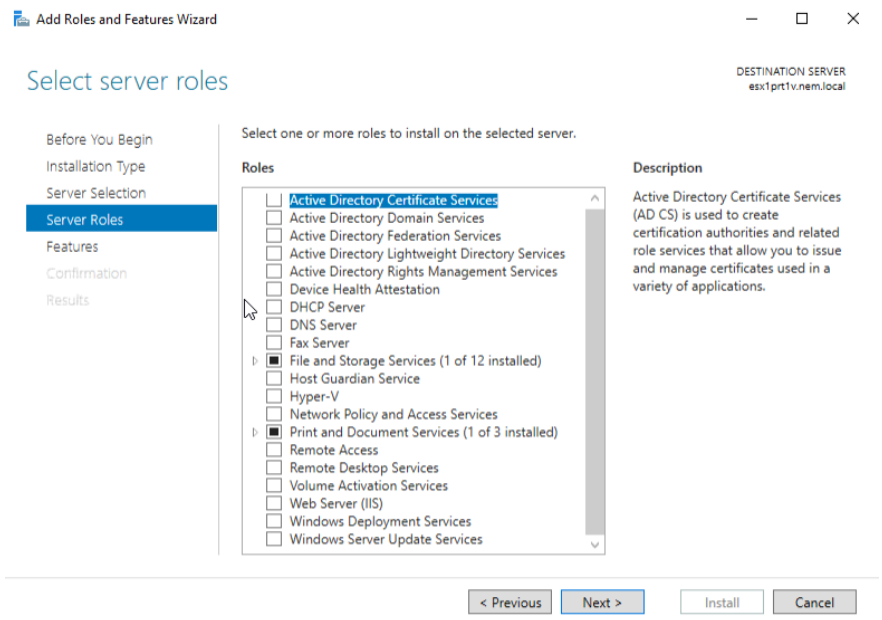
Zde již nebudeme opakovat postup pro vytvoření virtuálního stroje (esx1_prt1v) a základní instalaci, které je zmíněna v předchozích kapitolách, ale nakonfigurujeme IP adresu nyní již vytvořeného serveru. Pro nás (192.168.230.4), pak již budeme postupovat stejně, jako v předchozích případech jen zvolíme název (esx1prt1v) a připojíme do domény.



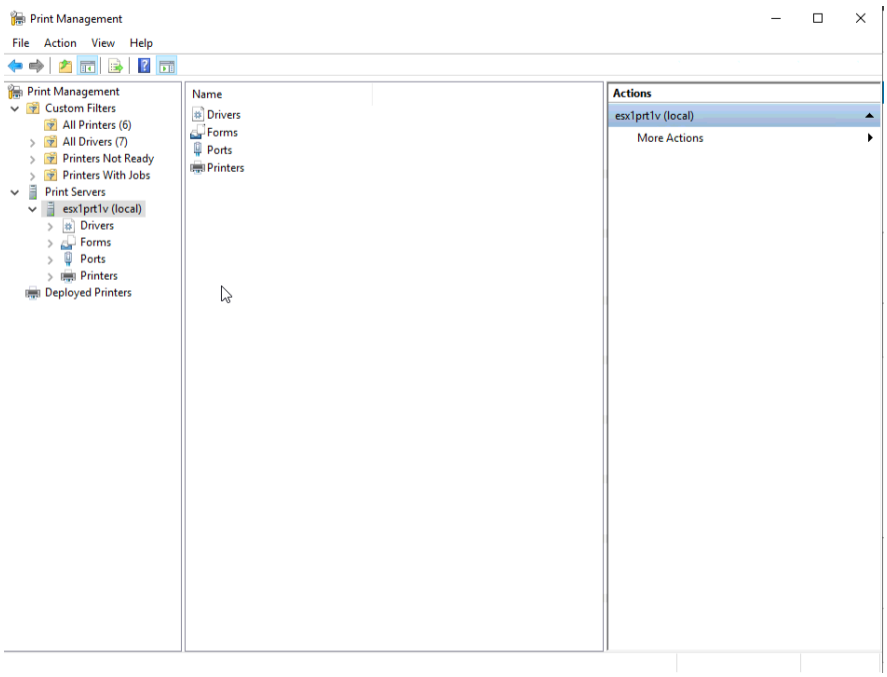
Obrázek 85 - Printserver síťový adaptér

10.2 Instalace služby

Pomocí Server manageru přidáme tiskové služby a dokončíme instalaci. Dále poté otevřeme nainstalovaný Print management, kde ovšem vzhledem k teoretické implementaci tiskárny nebudeme provádět žádné změny.



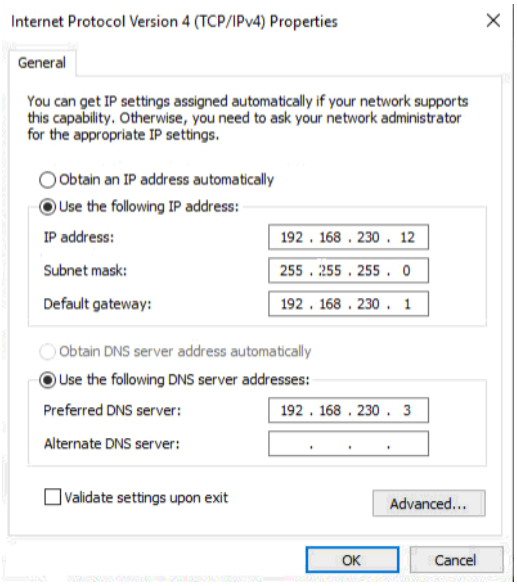
Obrázek 86 - Printserver konfigurace



Obrázek 87- Printserver konfigurace č.2

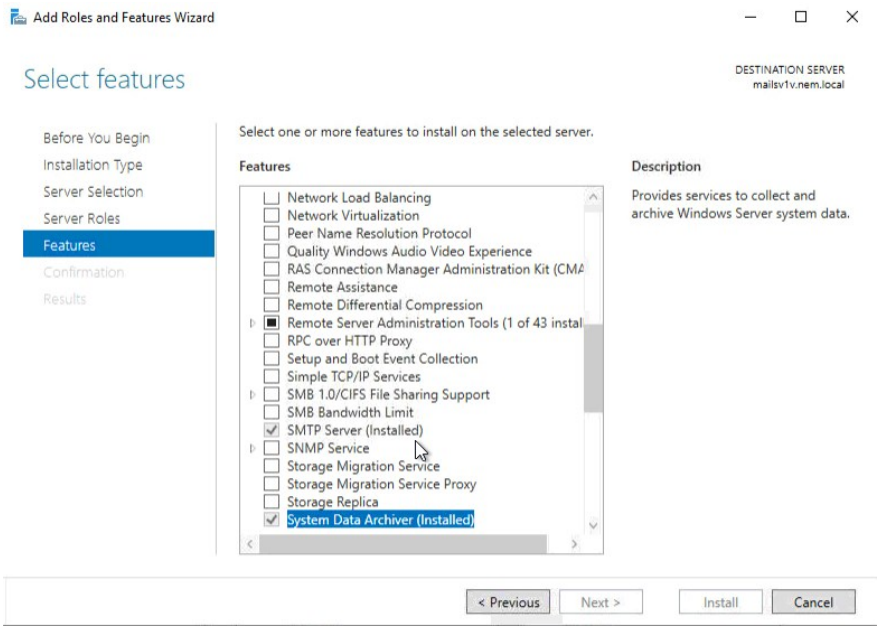
11 INSTALACE EMAILOVÉHO SERVERU

Proces počáteční instalace zůstává prozatím stejný, a proto se přesuneme rovnou ke konfiguraci síťové karty a instalaci konkrétních služeb. Nastavíme statickou IP adresu (192.168.230.12) a náš DNS server (192.168.230.3), zvolíme jméno stroje (mailsv1v) a připojíme do domény.



Obrázek 88 - Email server síťový adaptér

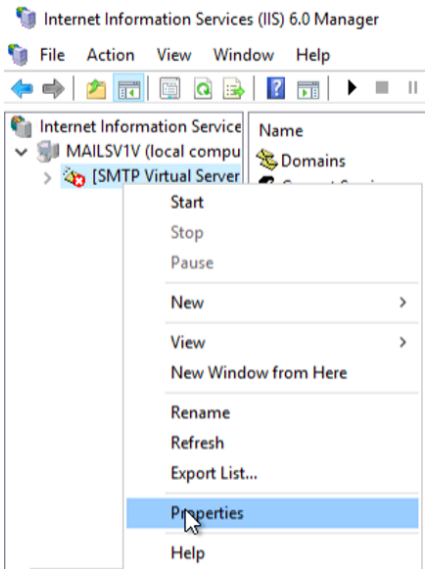
Přeskočíme serverové role, ve výběru jednotlivých funkcionalit zvolíme SMTP Server, avšak samotná instalace SMTP zvolí další nezbytné součásti v podobě omezené instalace webového serveru.



Obrázek 89 - Email server konfigurace

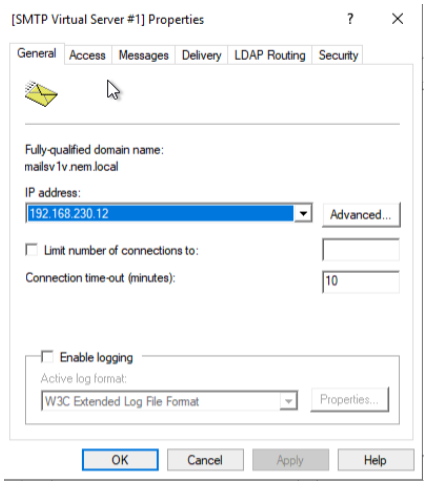
11.1 Konfigurace SMTP

Po dokončení instalace začneme s konfigurací SMTP služby. Otevřeme Internet Information Services (IIS) 6.0 Manager, kde již máme vytvořený virtuální SMTP server. Pravým tlačítkem vybereme Properties.

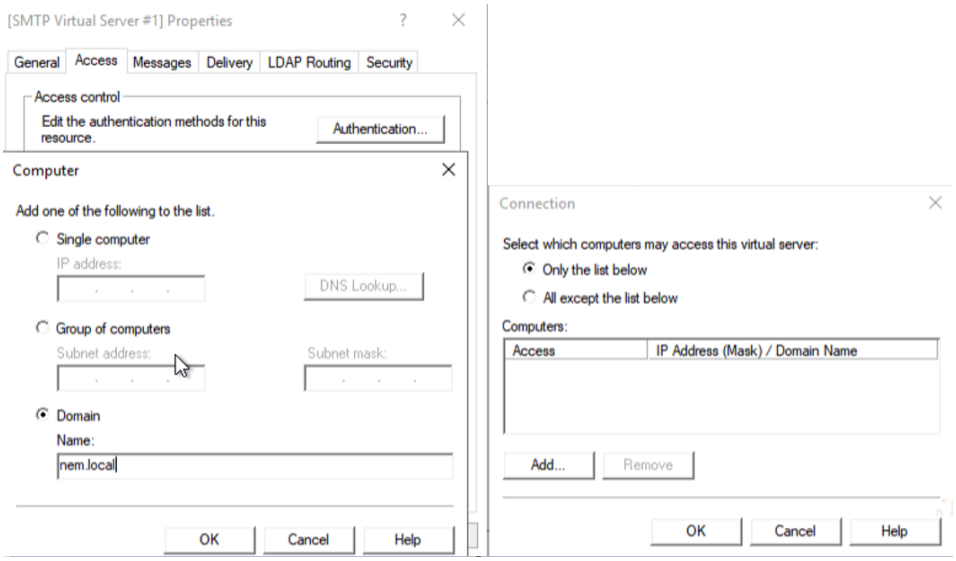


Obrázek 90 - Konfigurace SMTP

Dále pak nastavíme IP adresu serveru. V liště Access následně nastavíme, ze kterých subnetů (Vlan) bude možné se na server připojit. Lze zvolit cestu zavedení několika povolených, anebo naopak povolit všechny kromě zadaných. My povolíme pouze přístup z naší domény nem.local.

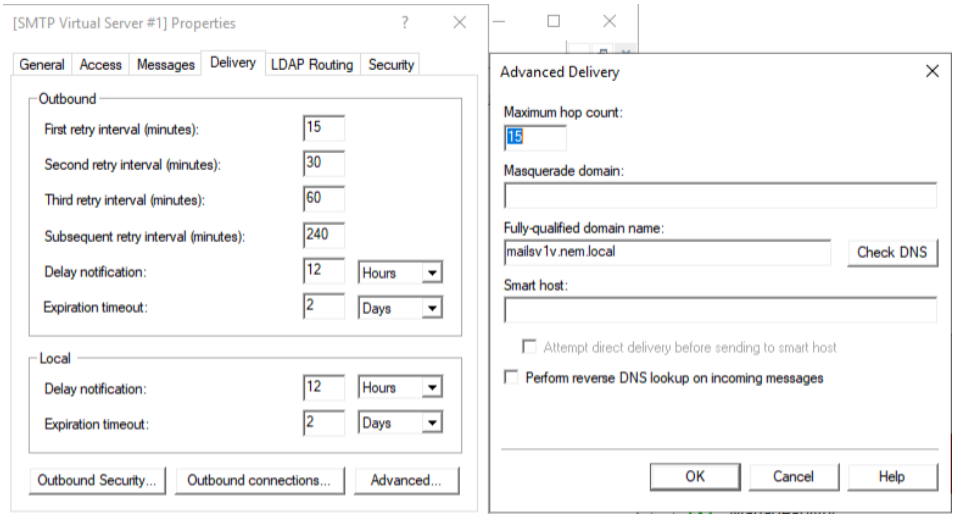


Obrázek 91 - Konfigurace SMTP č.2



Obrázek 92 - Konfigurace SMTP č.3

Poté zvolíme lištu Delivery a tlačítko Advanced, kde nastavíme doménové jméno našeho serveru a můžeme vyzkoušet funkčnost vůči DNS.



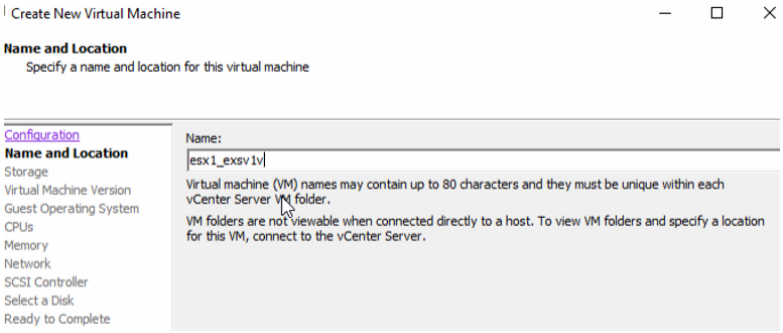
Obrázek 93 - Konfigurace SMTP č.4

Samozřejmě náš server nebude fungovat bez spojení s Microsoft Exchange Serverem, nicméně vzhledem k finančním limitacím nebudeme plně zprovozňovat toto spojení, takže náš emailový server bude fungovat pouze na bázi teoretické. A v praxi by tedy sloužil jako prostředník mezi příjemcem emailu a servery poskytovatelů mailových služeb, jako jsou Google, Microsoft a další, které by byly mimo naši doménu. Nicméně abychom mohli demonstrovat budoucí funkčnost emailu, vytvoříme si stejným způsobem jako v kapitole 10, další virtuální stroj, který pojmenujeme esx1_exsv1v, kde posléze stejnou cestou

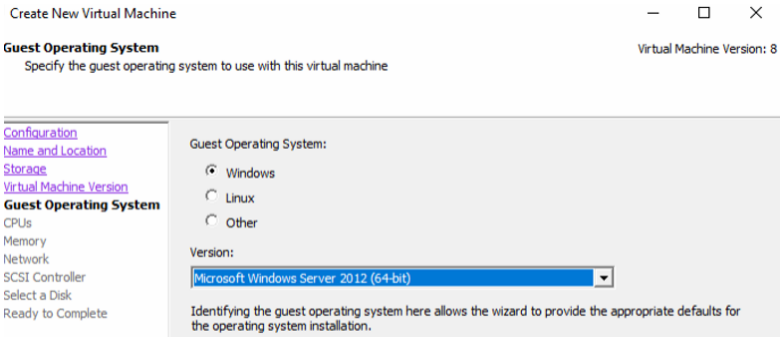
nainstalujeme a nastavíme Windows Server 2019 a poté nainstalujeme Windows Exchange Server, který si v evaluation verzi stáhneme z webu Microsoftu.

11.2 Instalace Exchange Serveru

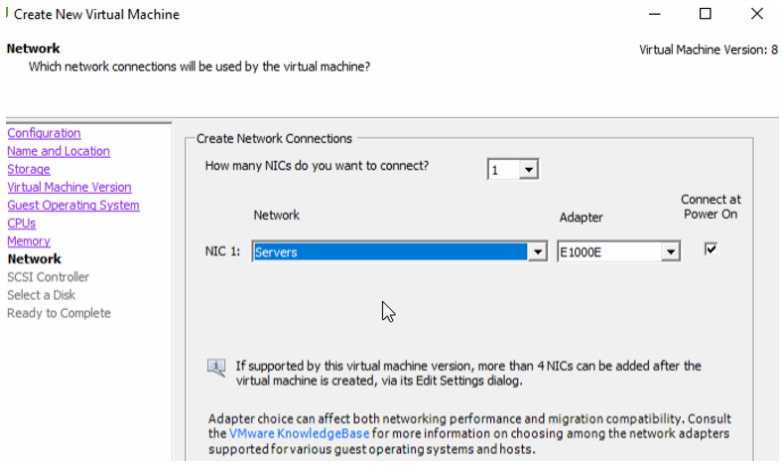
Vytvoříme si nový virtuální stroj (esx1_exsv1v) na který nainstalujeme operační systém, následně přiřadíme statickou IP adresu (192.168.230.11), doinstalujeme VMtools, připojíme Server do domény (exsv1v) a povolíme RDP stejně jako u SMTP serveru.



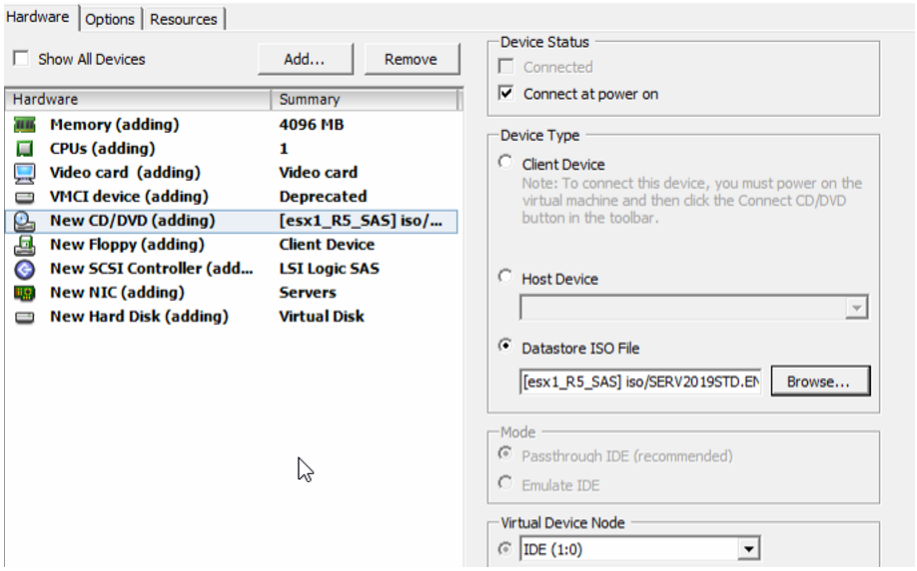
Obrázek 94 - Instalace Exchange serveru



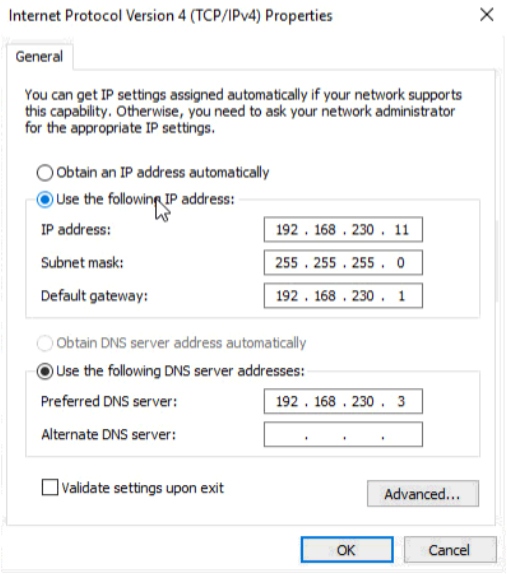
Obrázek 95 - Instalace Exchange serveru č.2



Obrázek 96 - Instalace Exchange serveru č.3

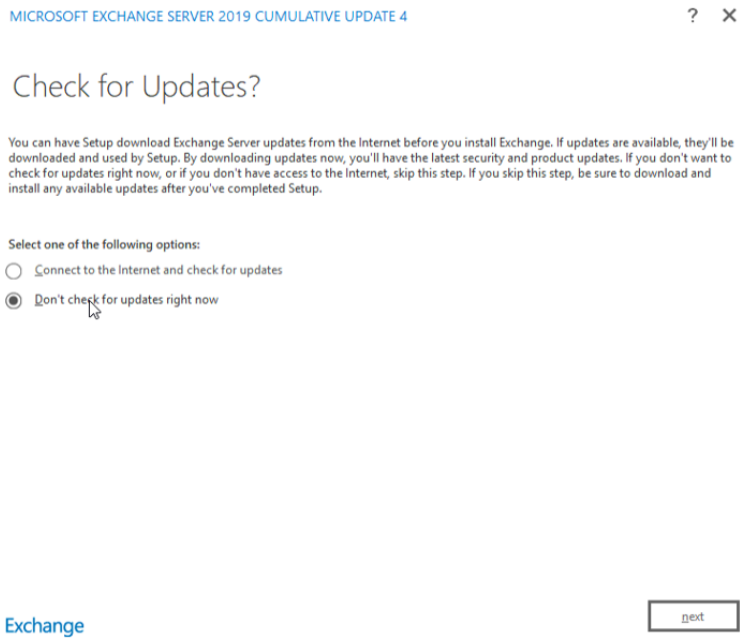


Obrázek 97 - Instalace Exchange serveru č.4

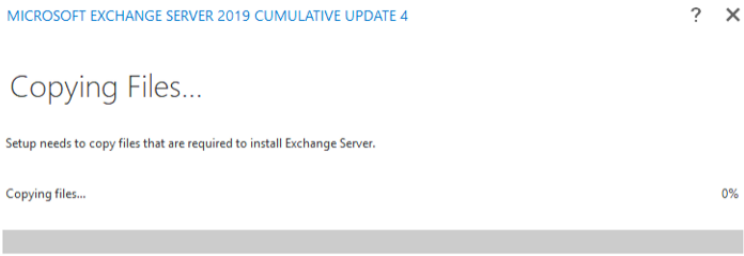


Obrázek 98 – Exchange server síťový adaptér

Po restartování serveru spustíme instalaci Exchange Serveru, nicméně předtím je nutné zkontrolovat, zda je uživatel, pod kterým spouštíme instalaci, v Active Directory skupinách (Domain Admins, Enterprise Admins a Schema Admins). Bez těchto skupin není možné server nainstalovat. Dále v průběhu instalace zvolíme neaktualizovat momentálně a počkáme, nežli se nakopírují data, které instalace potřebuje.

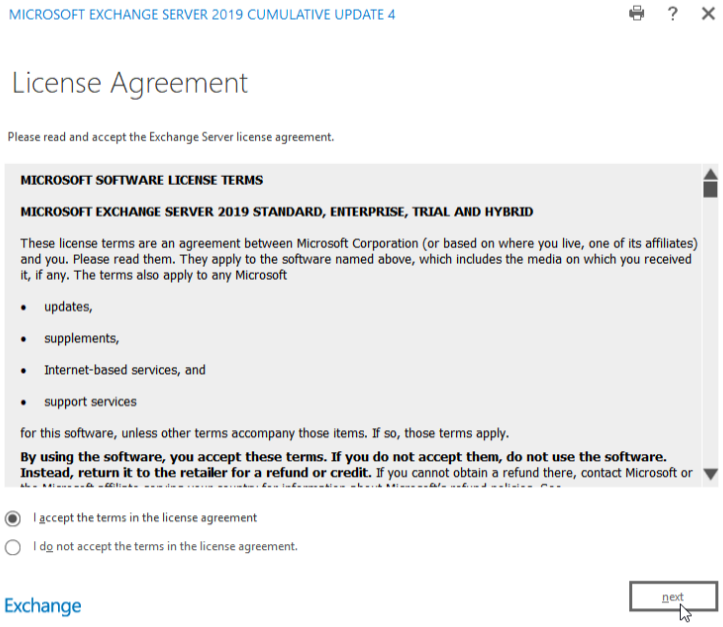


Obrázek 99 - Exchange server instalace č.5

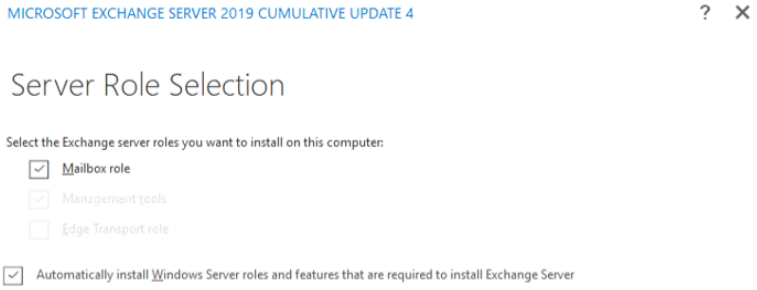


Obrázek 100 - Exchange server instalace č.6

V instalaci potvrdíme licenční ujednání, dále pak zvolíme roli našeho Exchange serveru, což bude role Mailboxu a taktéž vybereme, aby instalace nainstalovala všechny ostatní potřebné funkce a role Windows serveru.

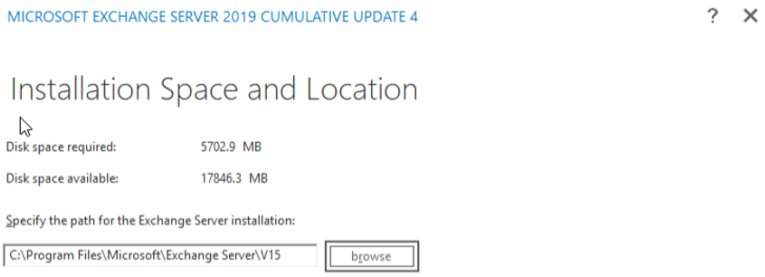


Obrázek 101- Instalace Exchange serveru č.7

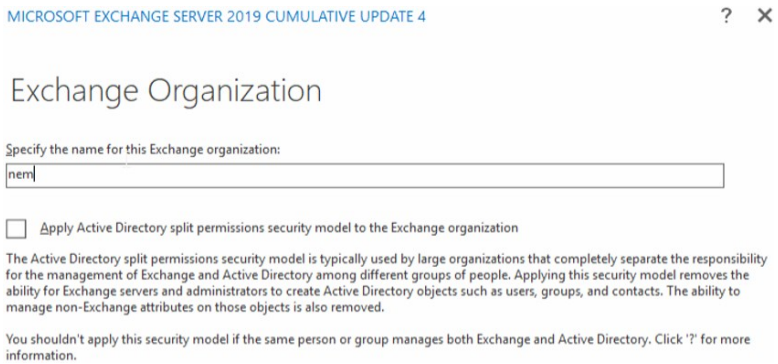


Obrázek 102 - Instalace Exchange serveru č.8

Posléze vybereme lokaci, kde se Exchange server nainstaluje a zvolíme jméno naší testovací organizace (nem).

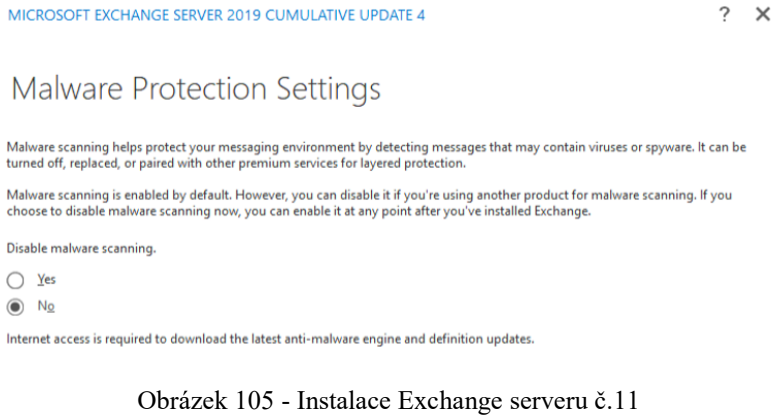


Obrázek 103 - Instalace Exchange serveru č.9

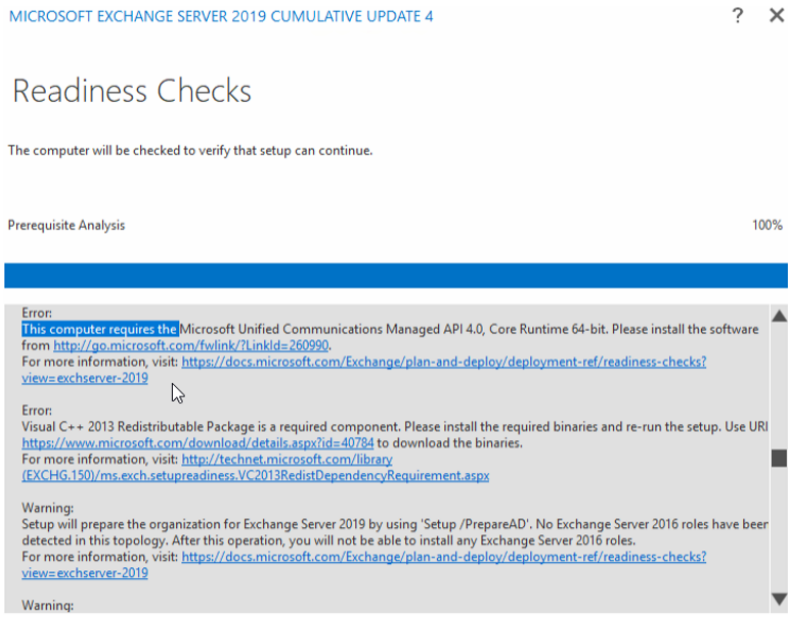


Obrázek 104 - Instalace Exchange serveru č.10

Na další straně se nás instalace zeptá, zda chceme vypnout skenování malwaru, což samozřejmě zvolíme ne. Na další straně již instalace kontroluje, zda máme na serveru nainstalované všechny prerekvizity a taktéž, jestli můžeme pokračovat v instalaci pod naším uživatelem.



Obrázek 105 - Instalace Exchange serveru č.11

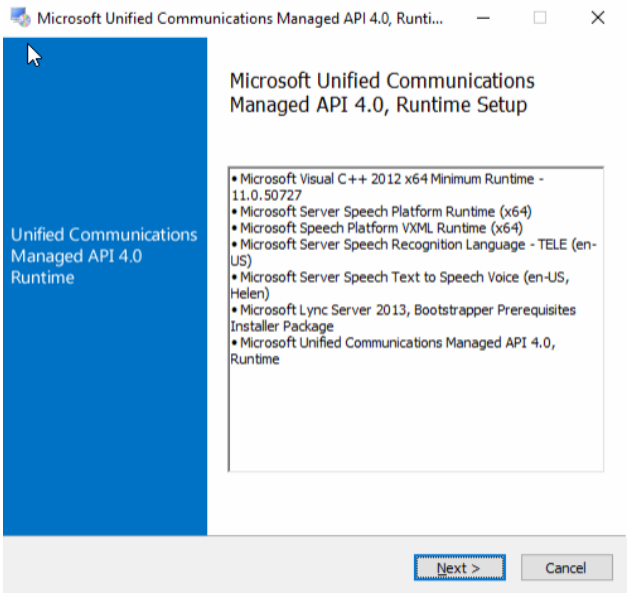


Obrázek 106 - Instalace Exchange serveru č.12

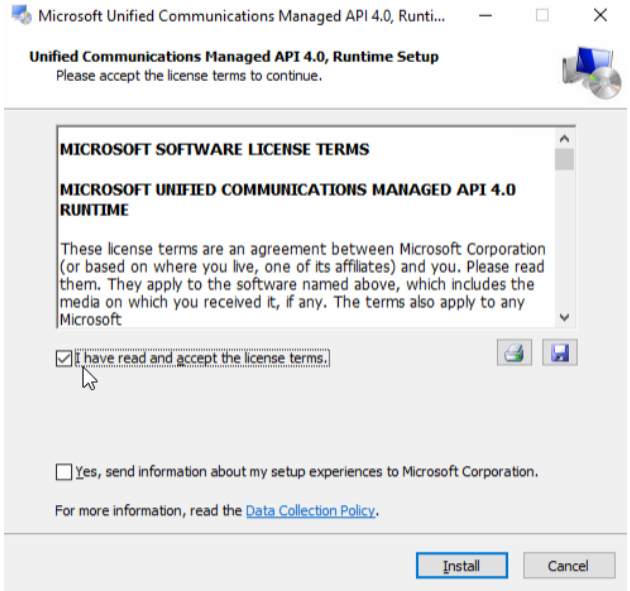
Nicméně v instalaci nám chybí několik bodů k pokračování, a tudíž nejdříve splníme tyto body.

11.2.1 Instalace prerekvizit

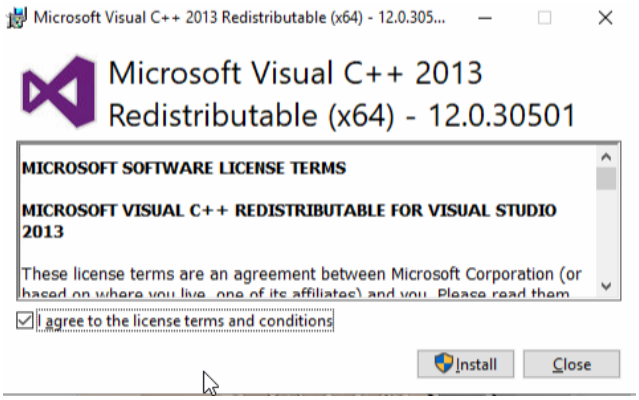
Prvně stáhneme Microsoft Unified Communitactions Managed API 4.0 (dostupné na https://www.microsoft.com/en-us/download/details.aspx?id=34992). Po stažení nainstalujeme a následně stáhneme Microsoft Visual C++ 2013 či novější verzi (dostupné z „https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads“) a taktéž nainstalujeme.



Obrázek 107 - Exchange server instalace prerekvizit



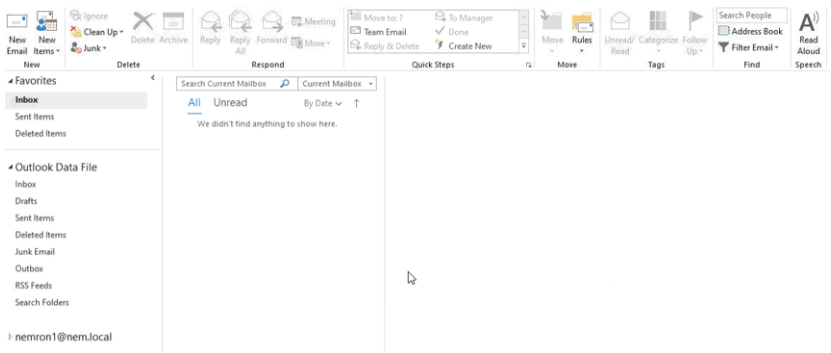
Obrázek 108 - Exchange server instalace prerekvizit č.2



Obrázek 109 - Exchange server instalace prerekvizit č.3

Nyní můžeme pokračovat v instalaci Exchange serveru. Instalace Exchange serveru nám bude fungovat jako ukázka funkčnosti emailové komunikace pouze na interní bázi, kdy v praxi bychom měli náš již vytvořený SMTP server a Exchange server hostovaný mimo naši doménu. Nyní stačí nainstalovat například Outlook z balíku O365 a připojit adresu k účtu.

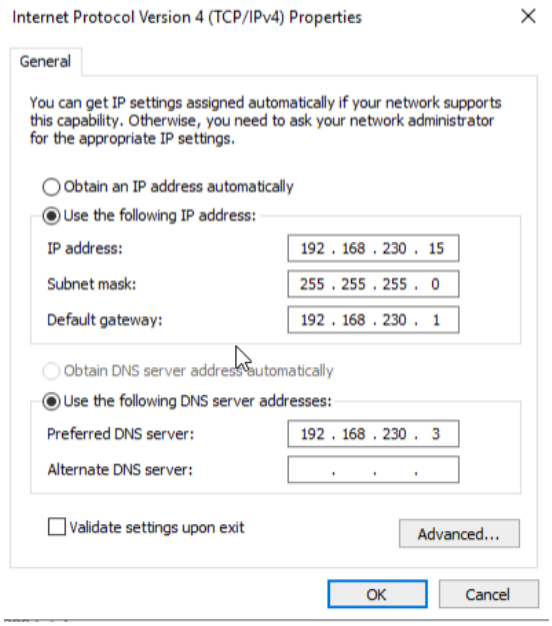
Obrázek 110 – Outlook



Obrázek 111 - Outlook č.2

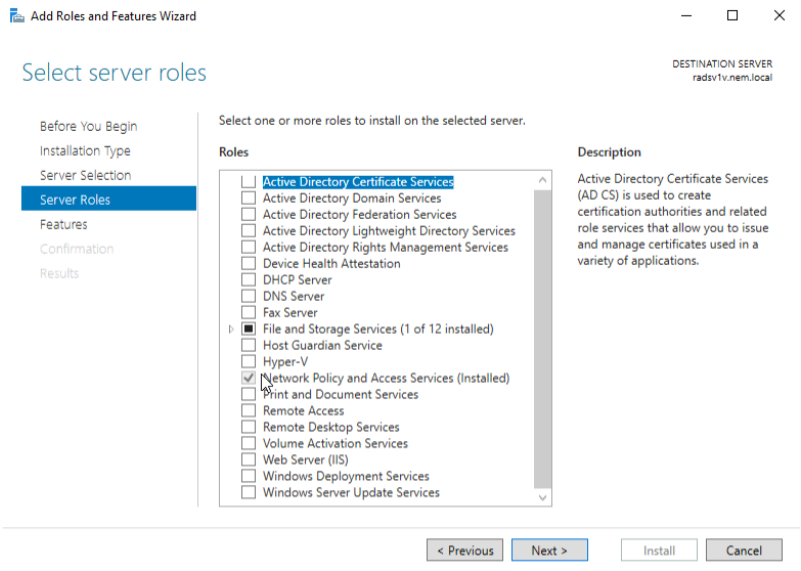
12 INSTALACE RADIUS SERVERU

Server nainstalujeme již pro nás standartní cestou, vytvoříme adekvátní název (radsv1v) a přiřadíme mu statickou IP adresu (192.168.230.15). Přidáme server do domény a zaktivujeme vzdálený přístup. Vše již bylo popsáno v předchozích kapitolách.



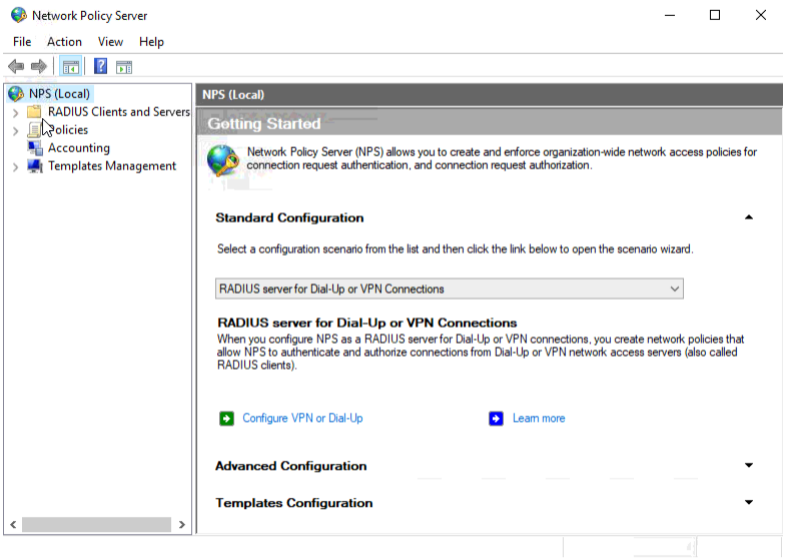
Obrázek 112 - Radius server síťový adaptér

V systémovém manažeru přidáme Network Policy and Access Services. Následně dokončíme instalaci, poté můžeme započít s konfigurací NPAS.

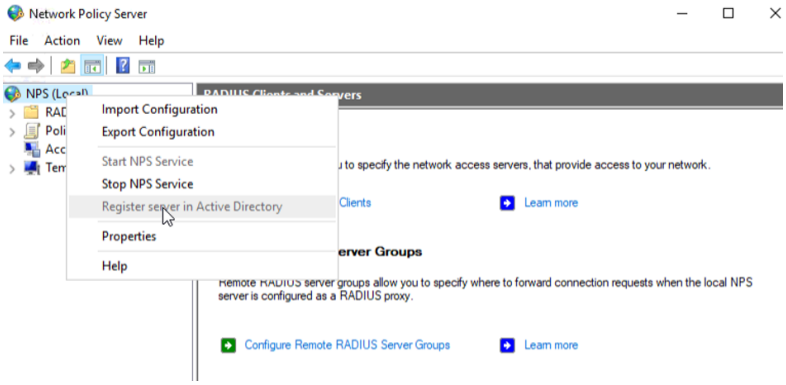


Obrázek 113 - Radius server konfigurace

Otevřeme si konzoli z nabídky Tools našeho Server Manageru. Kde je nejprve nutné autorizovat Radius server vůči Active Directory. Klikneme tudíž pravým tlačítkem na NPS (Local), kde vybereme Register server in Active Directory a potvrdíme registraci.

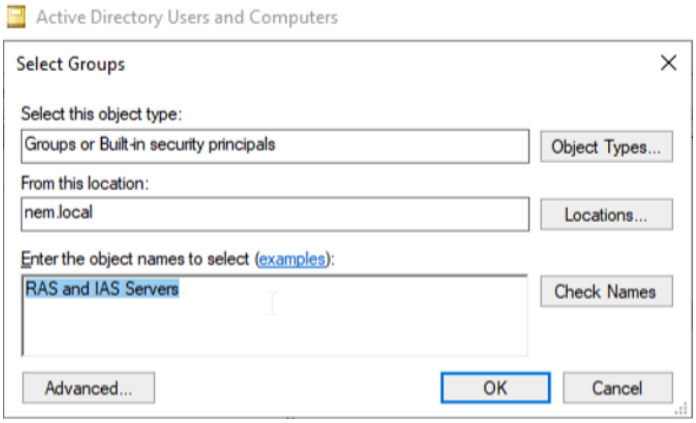


Obrázek 114 - Radius server konfigurace č.2



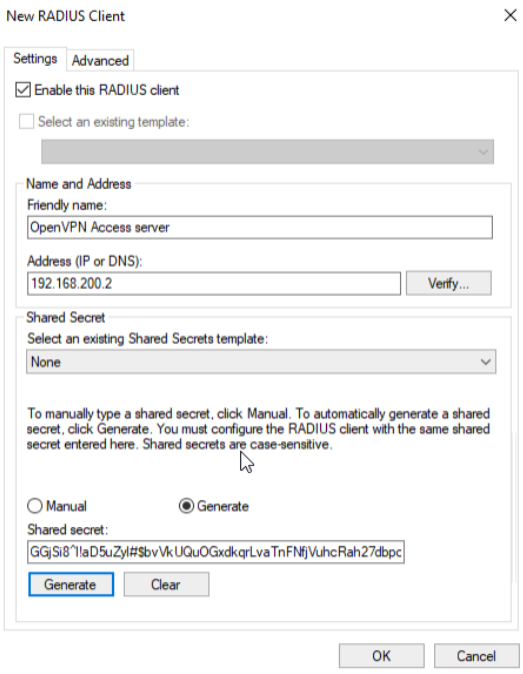
Obrázek 115 - Radius server konfigurace č.3

Server je potřeba přidat do již připravené skupiny v Active Directory na dc1v, a to konkrétně do RAS and IAS Servers, což našemu RADIUS server umožní zobrazovat a pracovat s parametry účtů, které se vážou (je jim umožněno používat) k VPN přístupu.



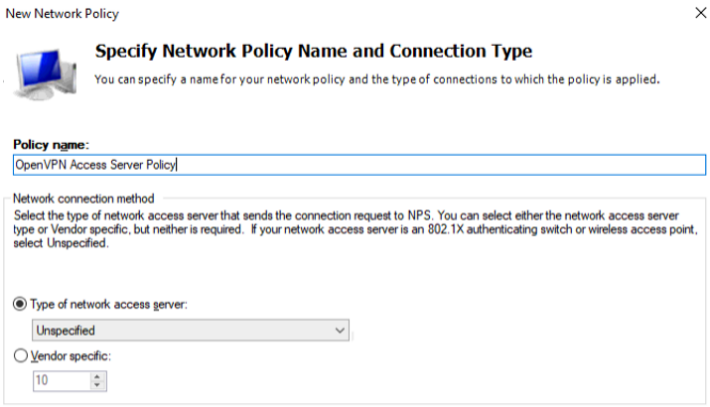
Obrázek 116 - Radius server konfigurace č.4

Následně již zase na radsv1v rozevřeme RADIUS Clients and Servers a pravým klikem na RADIUS Clients otevřeme nabídku a zvolíme New pro vytvoření RADIUS klienta. Kde doplníme do pole Friendly Name (vzhledem k následnému využití OpenVPN serveru pro VPN připojení) název OpenVPN Access Server. Doplníme IP adresu našeho VPN serveru, což je 192.168.200.2. A zvolíme Generate a následně vygenerujeme Shared Secret, který si musíme zkopírovat pro další nastavení.



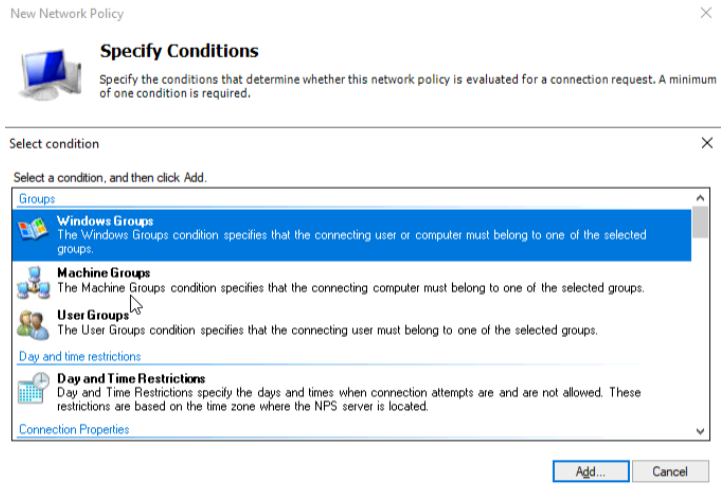
Obrázek 117 - Radius server konfigurace č.5

Po vytvoření klienta je potřeba nastavit síťové politiky, otevřeme si proto Policies/Network policies, pomocí pravého tlačítka na myši vytvoříme novou politiku, pojmenujeme ji OpenVPN Access Server Policy a dáme pokračovat.



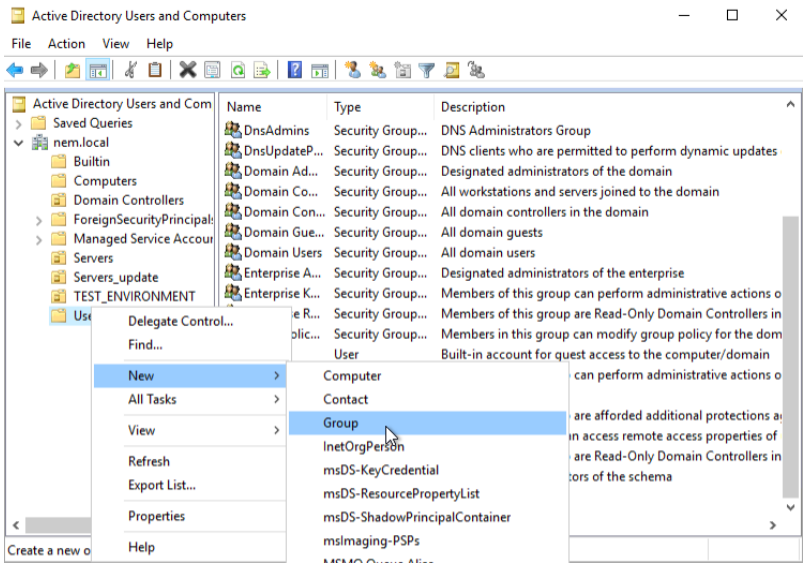
Obrázek 118 - Radius server konfigurace č.6

Na další straně přidáme pomocí Add, podmínky pro tuto politiku, zvolíme Windows Groups.

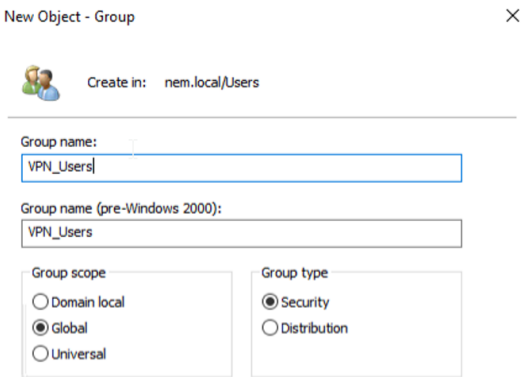


Obrázek 119 - Radius server konfigurace č.7

Po zvolení Windows Groups se nám otevře přidání konkrétních AD skupin. Předtím než skupinu přidáme, ji musíme vytvořit v Active Directory. Takže se připojíme na Domain Controller server a vytvoříme skupinu VPN_Users.

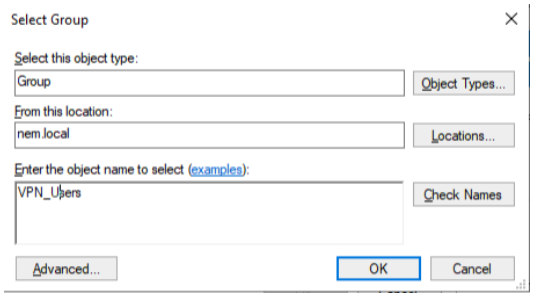


Obrázek 120 - Radius server konfigurace č.8



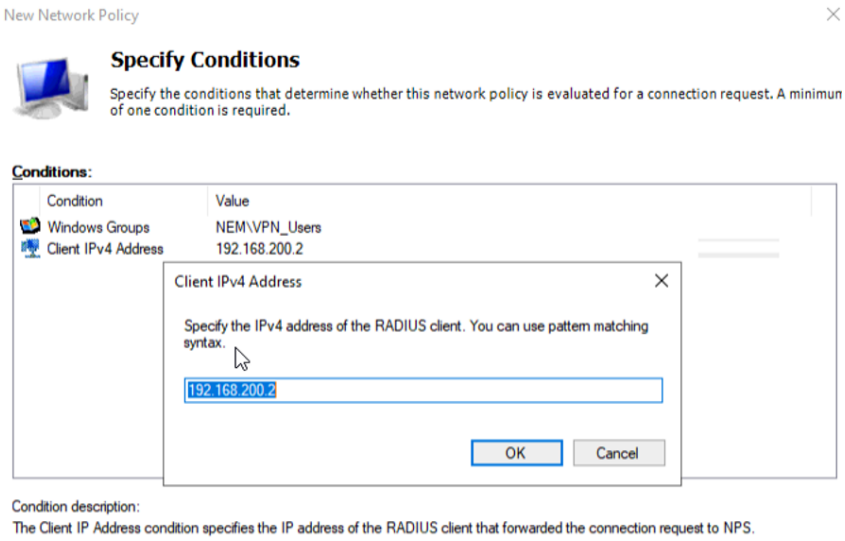
Obrázek 121 - Radius server konfigurace č.9

A nyní jsme schopni přidat skupinu do naší politiky na radsv1v.



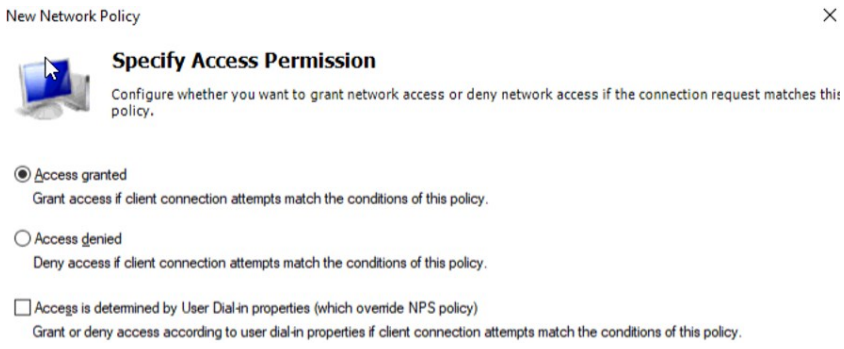
Obrázek 122 - Radius server konfigurace č.10

Nyní přidáme ještě další podmínku, a to IP adresu, odkud může server přijímat požadavky, což bude IP adresa našeho VPN serveru 192.168.200.2, čímž zamezíme přístupu ke zdrojům, které nejsou požadované.

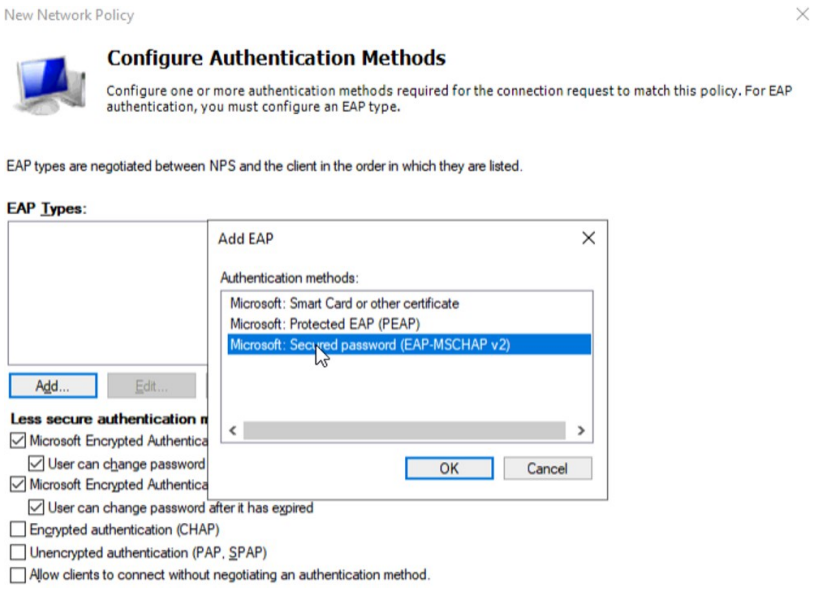


Obrázek 123 - Radius server konfigurace č.11

Dále již pak jen potvrdíme, že pakliže splní požadavek námi zvolené podmínky, pak bude přístup povolen. Na další straně pak přidáme protokol potřebný pro OpenVPN a to Microsoft Secured Password (EAP-MSCHAP v2) a poté již dokončíme konfiguraci.

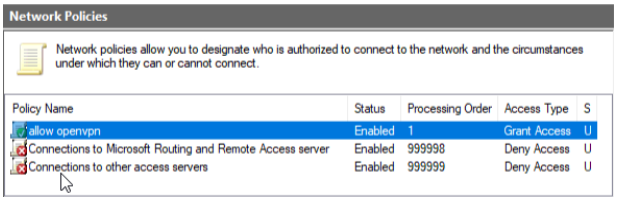


Obrázek 124 - Radius server konfigurace č.12



Obrázek 125 - Radius server konfigurace č.13

Naše vytvořená politika musí vždy v seznamu být nad defaultně vytvořenými politikami, aby byla v platnosti.



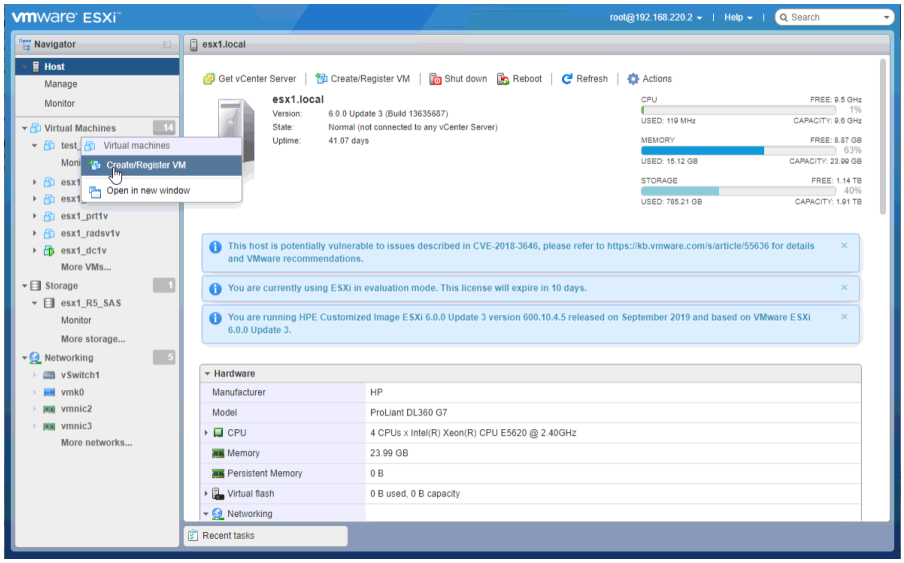
Obrázek 126 - Radius server konfigurace č.14

13 INSTALACE VPN SERVERU

Oproti zatím instalovaným serverům, budeme využívat OpenVPN server pro naše VPN služby, což znamená, že budeme instalovat server na bázi Linuxové distribuce. Tudíž bude instalace odlišná od instalování Windows Serveru, a to už při vytváření VM.

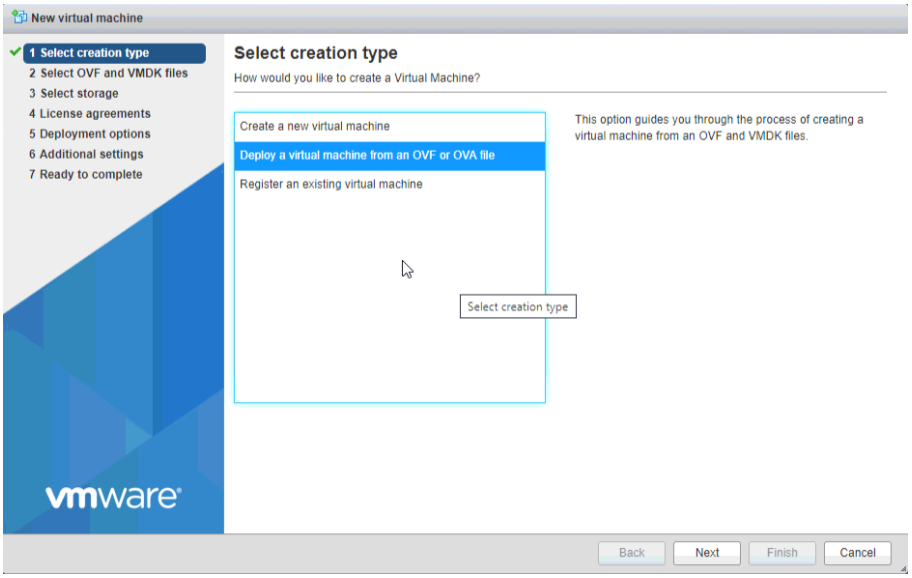
13.1 Příprava Virtuálního stroje

Nejprve musíme stáhnout správnou verzi systému OpenVPN, které jsou, jak již bylo zmíněno v teoretické části, na bázi Ubuntu, konkrétně verze 18.04 LTS x64 bez uživatelského rozhraní. Defaultně jsou systému přiřazeny 1GB paměti RAM a 1 jádro procesoru. Taktéž je předinstalován balíček opensource VM tools. Stažení verze systému provedeme pomocí odkazu: „https://openvpn.net/downloads/openvpn-as-latest-vmware.ova“. Po dokončení stahování zaregistrujeme nový VM, pomocí webového rozhraní nebo Vsphere klienta.



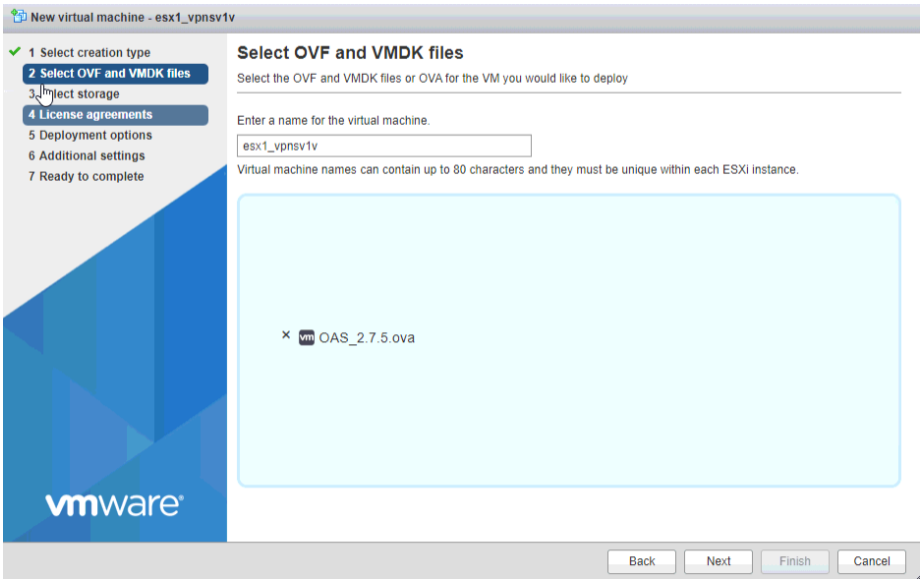
Obrázek 127 - Vytváření OpenVPN VM

V instalačním průvodci nezvolíme Create a new virtual machine jako doposud, nýbrž vybereme Deploy a virtual machine from an OVF or OVA file, protože připravený systém je ve formátu OVA.



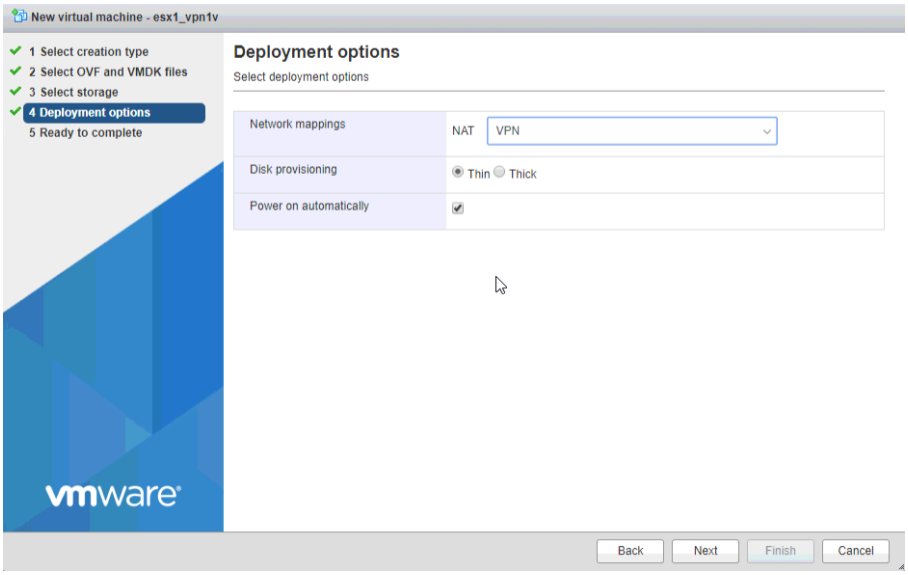
Obrázek 128 - Vytváření OpenVPN VM č.2

Následně zvolíme jméno stroje (pro nás esx1_vpnsv1v), a vyhledáme stažený soubor, který použijeme při instalaci, kdy jej můžeme vyhledat nebo použít Drag & Drop.



Obrázek 129 - Vytváření OpenVPN VM č.3

Dále zvolíme úložiště, které bude stejné jako u předchozích strojů a poté je potřeba zvolit síť (kterou již máme nachystanou z předchozích kapitol), kde vybereme VPN. Nyní je třeba vyčkat, než se vytvoří virtuální stroj a nahraje se připravený obraz systému OpenVPN, čímž pak bude náš virtuální stroj nachystaný pro následnou konfiguraci.



Obrázek 130 - Vytváření OpenVPN VM č.3

13.2 Konfigurace OpenVPN serveru

Prvotní přihlášení je root s heslem openvpnas, kdy ihned po přihlášení po nás server požaduje několik výběrů. Všechny budeme nechávat v defaultním stavu, a tudíž stačí jen potvrzovat.

```
OpenVPN Access Server Appliance 2.7.5 openvpnas2 tty1
openvpnas2 login: root
Password: _
```

Obrázek 131 - OpenVPN přihlášení

Defaultně systém počítá s DHCP serverem, který mu přiřadí dynamickou IP adresu, nicméně u nás bude serveru přiřazena statická adresa, a proto instalační průvodce zahlásí chybu (konkrétně IndexError: list index out of range).

```
Please specify the network interface and IP address to be
used by the Admin Web UI:
(1) all interfaces: 0.0.0.0
Please enter the option number from the list above (1-1).
> Press Enter for default [0]: 1
Traceback (most recent call last):
  File "/usr/local/openvpn_as/bin/_ovpn-init", line 422, in <module
    LOGIN_IP = SUGGEST_IPS[1]
IndexError: list index out of range
root@openvpnas2:~# _
```

Obrázek 132 - Konfigurace defaultního síťového adaptéru

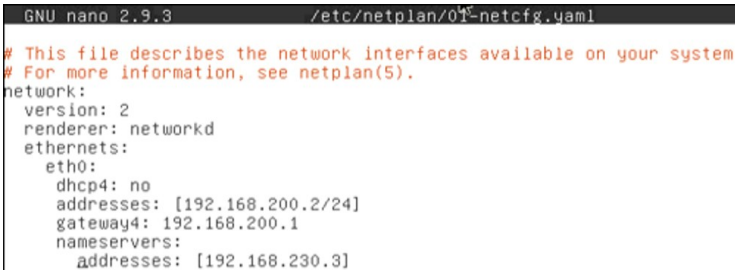
Nyní je potřeba upravit konfigurační soubory serveru tak, že budeme moc přiřadit statickou IP adresu, masku sítě i bránu a následně přidáme i náš DNS server. Zvolíme si textový editor pro úpravu daných souborů, pro nás to bude editor nano. Příkazem „nano /etc/netplan/01-netcfg.yaml“ otevřeme tento konfigurační soubor. [18]

Obrázek 133 - Úprava netcfg.yaml

Zde upravíme defaultní konfiguraci, a to následovně. Na řádku obsahujícím dhcp4 upravíme hodnotu na „no“. A následně se posuneme na další řádek a zadáme:

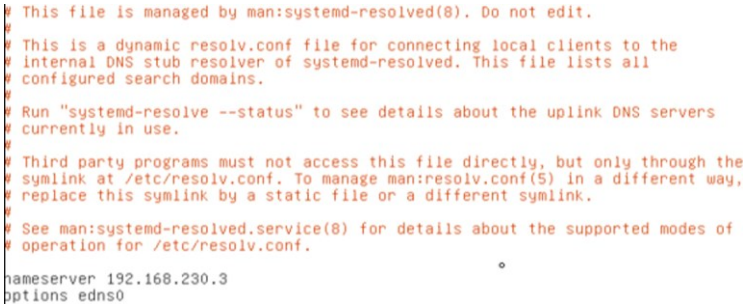
- addresses: [192.168.200.2/24]
- gateway4: 192.168.200.1
- nameservers:
  - addresses: [192.168.230.3]

Je nutné dodržet stylistickou úpravu, jinak konfigurace nebude považována za správnou. Následně uložíme zadané hodnoty pomocí klávesové zkratky „Ctrl + s“ a poté opustíme nano editor pomocí „Ctrl + x“. [18]



Obrázek 134 - Úprava netcfg.yaml č.2

Nyní pomocí příkazu „netplan apply“ aplikujeme námi zadané hodnoty. Dále je nutné ještě aplikovat změny v konfiguraci DNS. Poté otevřeme příkazem „nano /etc/resolv.conf“ a upravíme hodnotu „nameserver:“ na 192.168.230.3, což je IP adresa našeho DNS serveru. Volbu uložíme opět pomocí „Ctrl + s“ a opustíme editor pomocí „Ctrl + x“. [27]



Obrázek 135 - Změna nameserveru

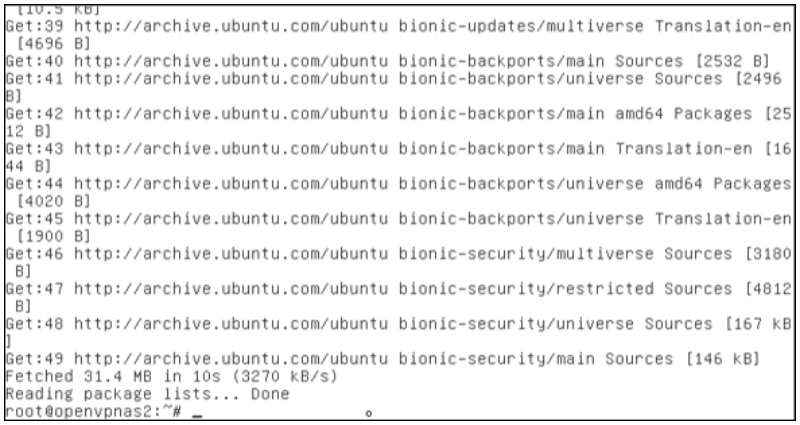
Nyní máme nastavený síťový přístup pro server, ale ještě je potřeba změnit heslo pro administrátorský účet root, neboť bez změny by byl velmi rychle zneužitelný. Pomocí příkazu „passwd“ změníme heslo na námi požadované heslo vysoké odolnosti. Dále je potřeba aktualizovat přístupový server na poslední verzi pomocí příkazu: „wget https://openvpn.net/downloads/openvpn-as-latest-ubuntu18.amd_64.deb“.

Obrázek 136 - Aktualizace Linux distribuce

Dále aktualizujeme operační systém OpenVPN pomocí dvou příkazů a to:

- apt-get update
- apt-get upgrade

A dvakrát potvrdíme využití dalšího prostoru balíčku na disku a instalaci údržbového klávesou „y“, což značí „yes“.



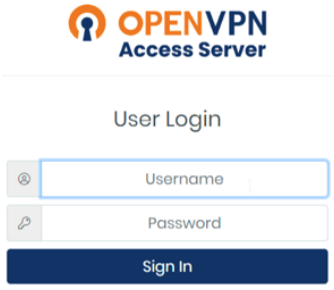
Obrázek 137- Aktualizace Linux distribuce č.2

Obrázek 138 - Aktualizace Linux distribuce č.3

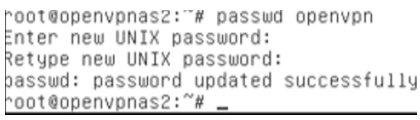
Po dokončení aktualizace je ještě potřeba nastavit místní časové pásmo pomocí příkazu: „dpkg-reconfigure tzdata “, kde následně vybereme Europe/Prague. Nyní je možné otevřít webový interface našeho VPN serveru a to na námi zadané adrese na portu 943 „192.168.200.2:943/Admin“. [27]

Obrázek 139 - Změna časového pásma

Kde se můžeme přihlásit pomocí prvotního účtu openvpn, pro který ještě v konzoli změníme heslo pomocí příkazu: „passwd openvpn“, kde na dalším řádku zvolíme nové heslo a poté ho zopakujeme. [18]



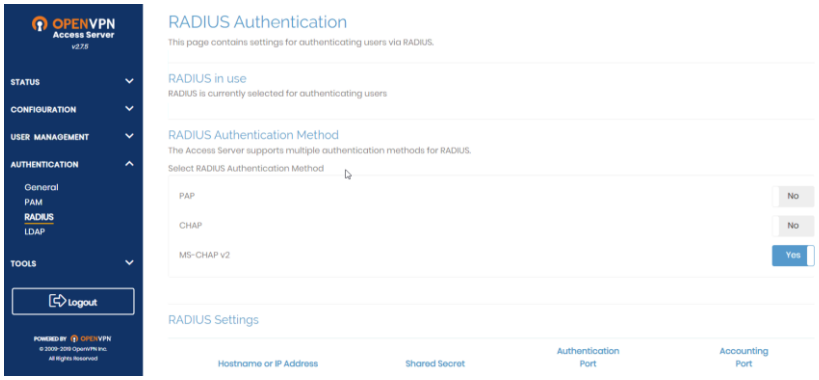
Obrázek 140 - OpenVPN přihlášení



Obrázek 141 - Změna hesla pro openvpn uživatele

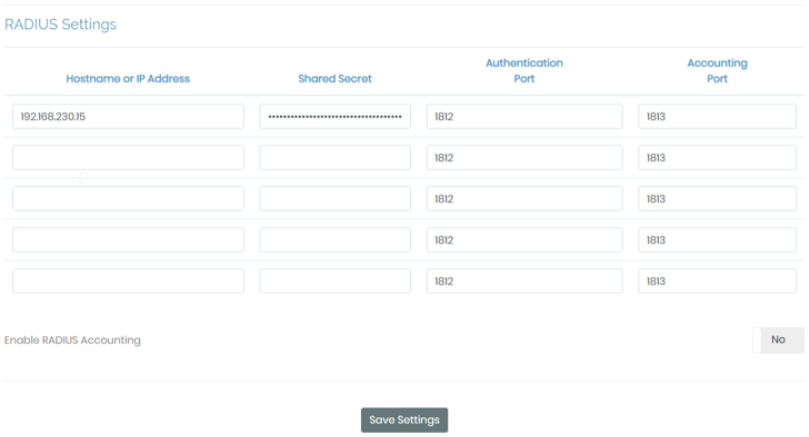
13.3 Nastavení autentifikace a dokončení konfigurace

Pro umožnění připojení přes VPN, jsme nejprve v kapitole 11. na našem DC serveru vytvořili v Active Directory novou skupinu pro uživatele, kteří budou mít možnost VPN používat. Pojmenovali jsme ji VPN_Users. Následně jsme přidali náš účet nemron1 do skupiny. Dále jsme na Radius serveru (radsv1v) v NPS (Network policy server) přidali nového klienta a řádně nastavili. Nyní nám již zbývá nakonfigurovat samotný VPN server, neboť RADIUS a další prerekvizity máme nachystané. Přihlásíme se jako administrátor na VPN webový interface (192.168.200.2:943/Admin) a zvolíme možnost Authentication, kde vybereme RADIUS. Zvolíme MS-CHAP v2 a potvrdíme používání RADIUS autentifikace (pro restart služeb na serveru a rekonfiguraci). [18]



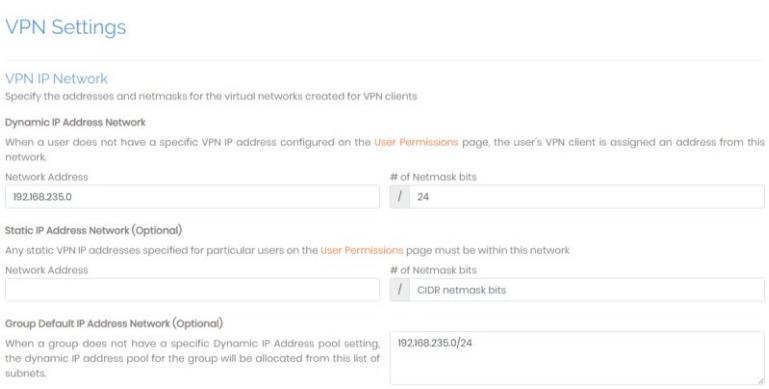
Obrázek 142 - Konfigurace OpenVPN

Dále přidáme náš RADIUS server do databáze a přiřadíme k němu Shared Secret, který jsme zvolili při konfiguraci radsv1v.

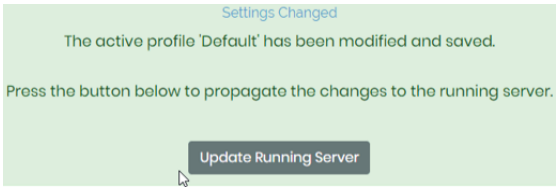


Obrázek 143 - Konfigurace OpenVPN č.2

Nyní vybereme Configuration a zde zvolíme VPN Settings, změníme Dynamic IP Address Pool na 192.168.235.0 s maskou /24 a restartujeme server pomocí Update running server, což se nám ukáže po uložení změn.

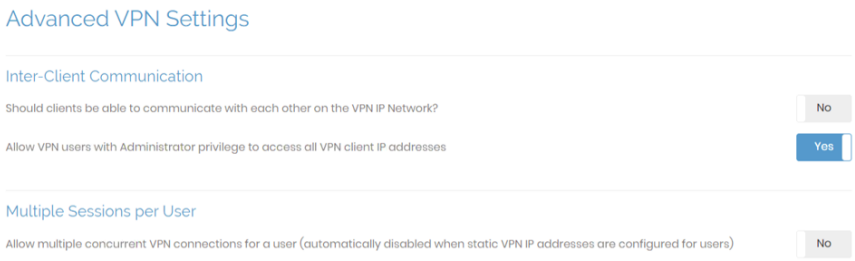


Obrázek 144 - Konfigurace OpenVPN č.3



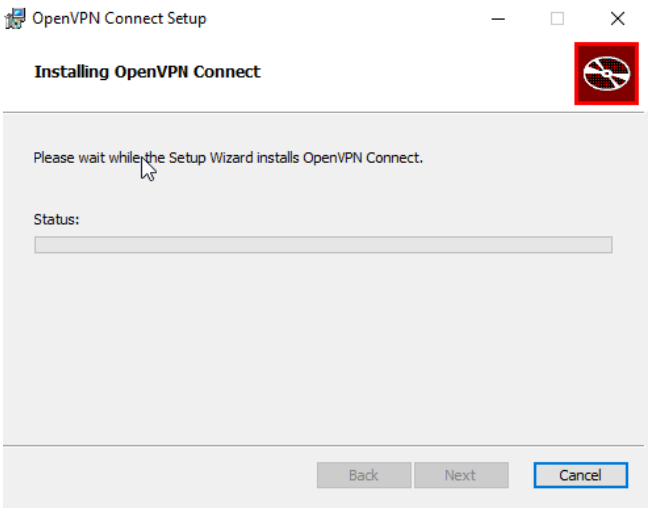
Obrázek 145 - Konfigurace OpenVPN č.4

Následně se posuneme do Menu Advanced VPN, kde změníme možnosti pro vícero připojení pro jednoho uživatele na „NO“ a povolíme Administrátorům přístup na klientské IP adresy (zvolením „YES“).



Obrázek 146 - Konfigurace OpenVPN č.5

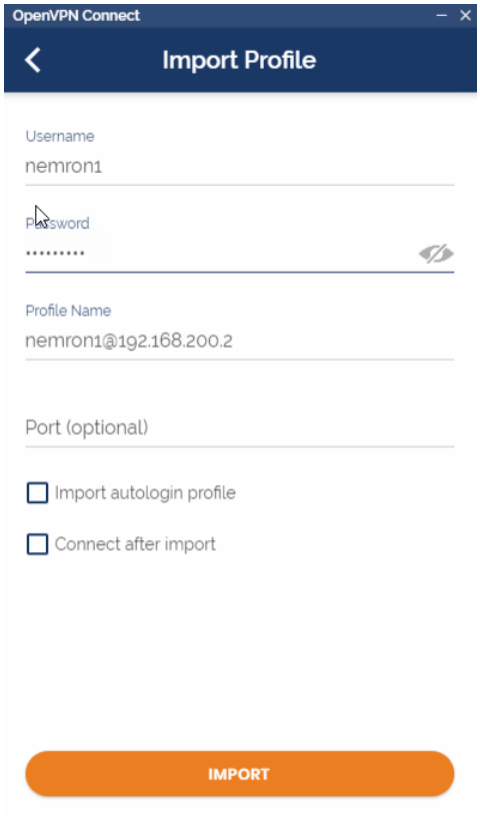
Dále již jen stáhneme na klientský pc openVPN client software (dostupný z https://openvpn.net/client-connect-vpn-for-windows/), který nainstalujeme na klientský pc. V průběhu instalace nic neměníme a posléze program spustíme. Po spuštění je potřeba naimportovat profil, což se bude skládat z url adresy našeho vpn serveru (192.168.200.2) a poté údajů pro přihlášení do Windows, které nám poskytne AD a ověří Radius server. Profil naimportujeme a poté lze vytvořit odkaz přímo pro připojení nebo se manuálně připojit. [18]



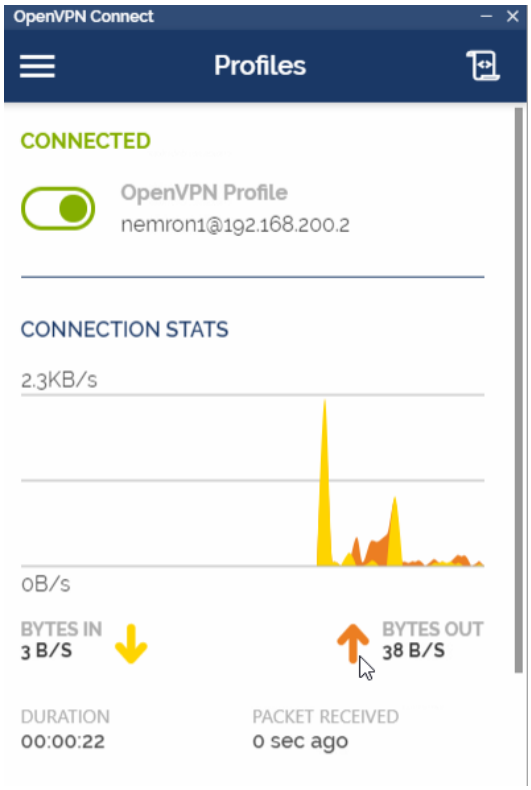
Obrázek 147 - Klient Instalace OpenVPN

Obrázek 148 - Klient Import OpenVPN

profilu



Obrázek 149 - Import OpenVPN profilu č.2

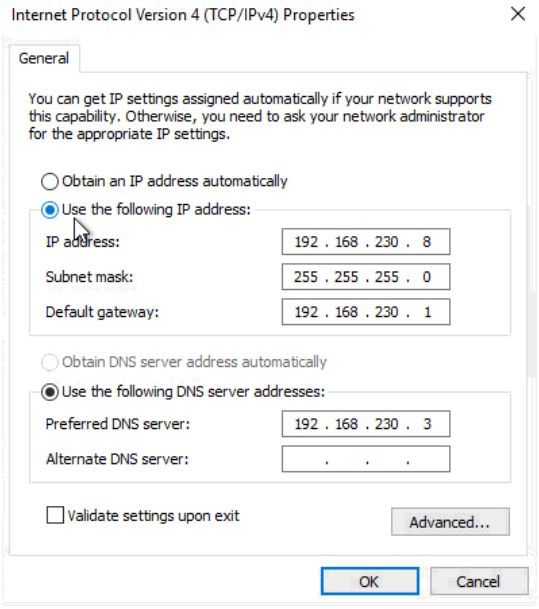


Obrázek 150 - Test konektivity OpenVPN

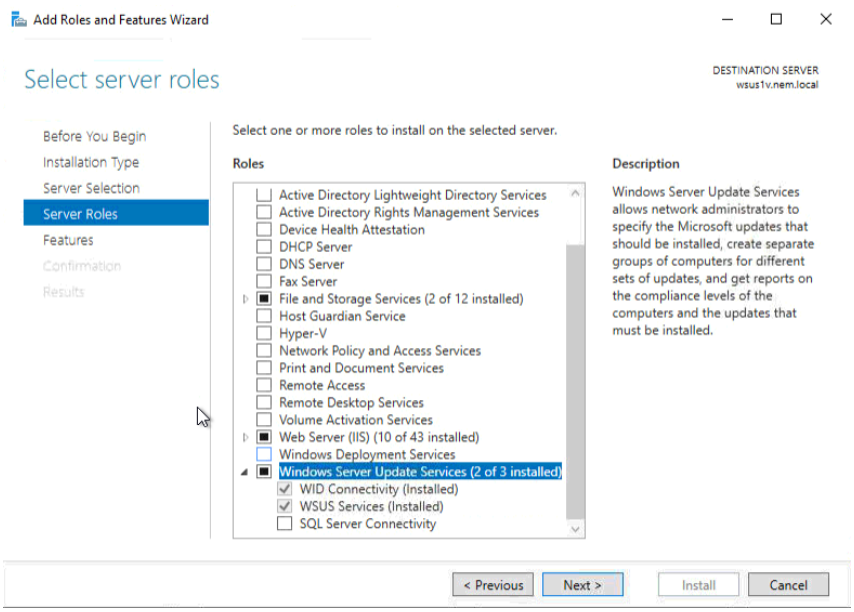
Obrázek 151 - OpenVPN připojení

14 INSTALACE SERVERU WSUS

Základní vytvoření VM a instalaci serveru WSUS provedeme stejně jako u předchozích serverů. Zvolíme název esx1_wsus1v pro virtuální stroj. Přidáme do port skupiny Servers a následně spustíme instalaci. Po nainstalování Windows zadáme serveru statickou IP adresu (192.168.230.8) a název (wsus1v), následně povolíme RDP připojení, nainstalujeme VMware tools a připojíme server do domény (nem.local), aby byla práce se serverem jednodušší.

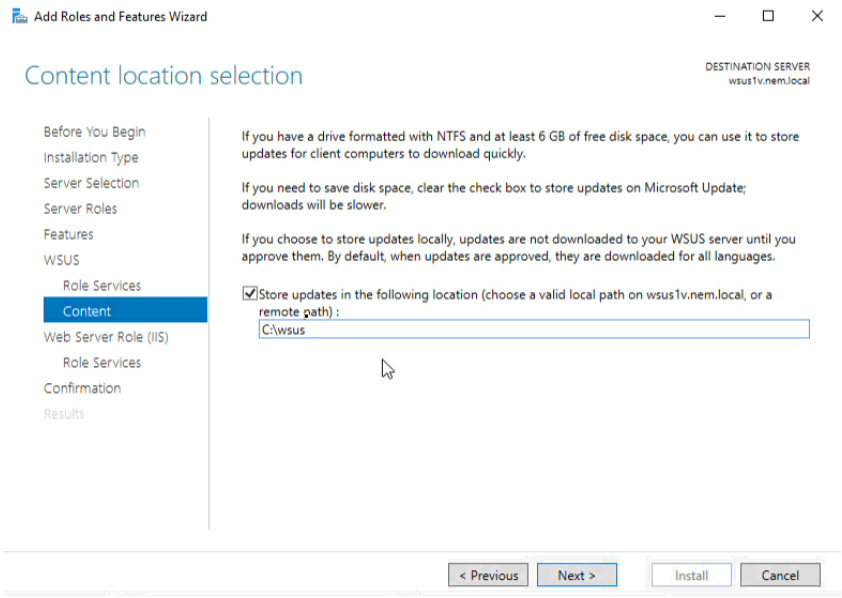


Obrázek 152 - WSUS server síťový adaptér

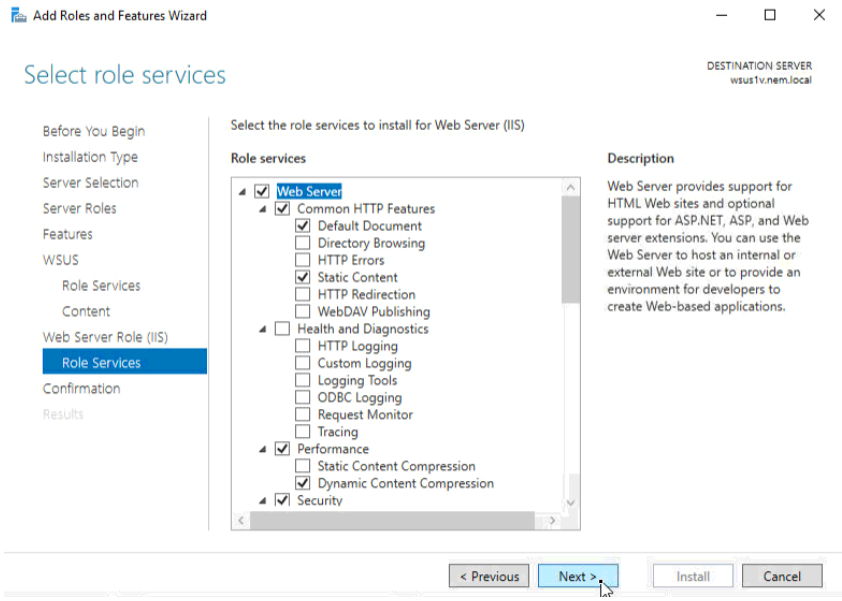


Obrázek 153 - WSUS server konfigurace

V Server Manageru přidáme Windows Server Update Services, které si automaticky přidají IIS webový server, ale jen součásti potřebné pro WSUS funkce. Dále pokračujeme beze změn v instalačním průvodci. Až na listu Content, zvolíme složku, kam se budou dostupné aktualizace ukládat (vytvoříme C:\data). Instalaci dokončíme, poté klikneme na Launch Post-installation tasks, dokončíme a můžeme začít konfigurovat naši WSUS službu.



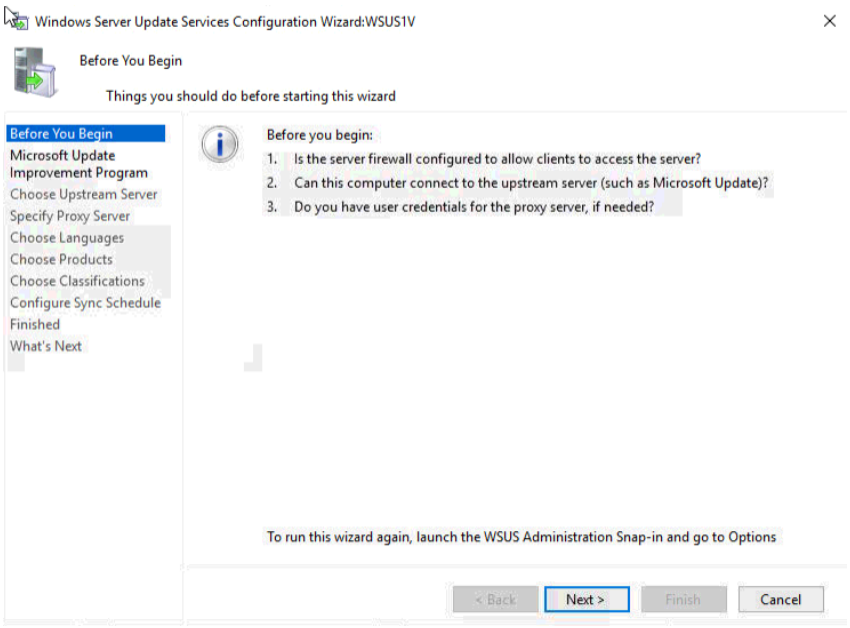
Obrázek 154 - WSUS server konfigurace č.2



Obrázek 155 - WSUS server konfigurace č.3

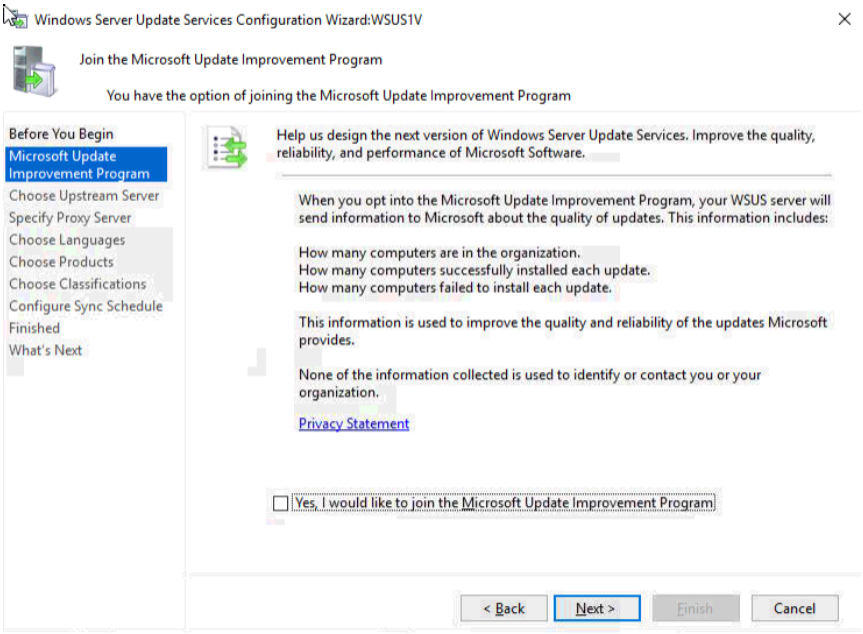
14.1 Konfigurace WSUS služby

Pomocí Tools v Server Manageru otevřeme Windows server update services, kde budeme pokračovat v konfiguraci služby.



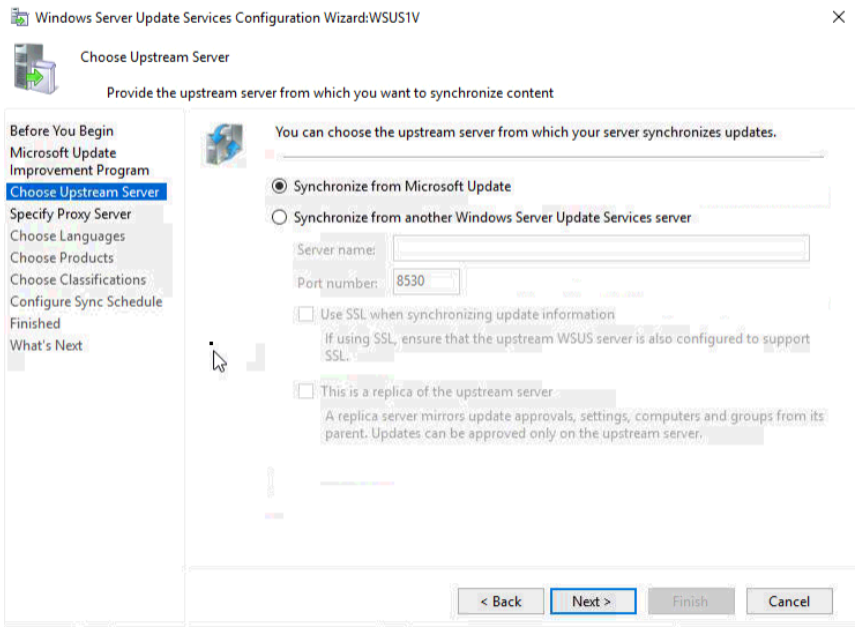
Obrázek 156 - Konfigurace WSUS služby

Po zvolení Next se dostáváme na další stranu, kde nezaškrtneme políčko souhlasu s připojením se do Microsoft Update Improvement Program.



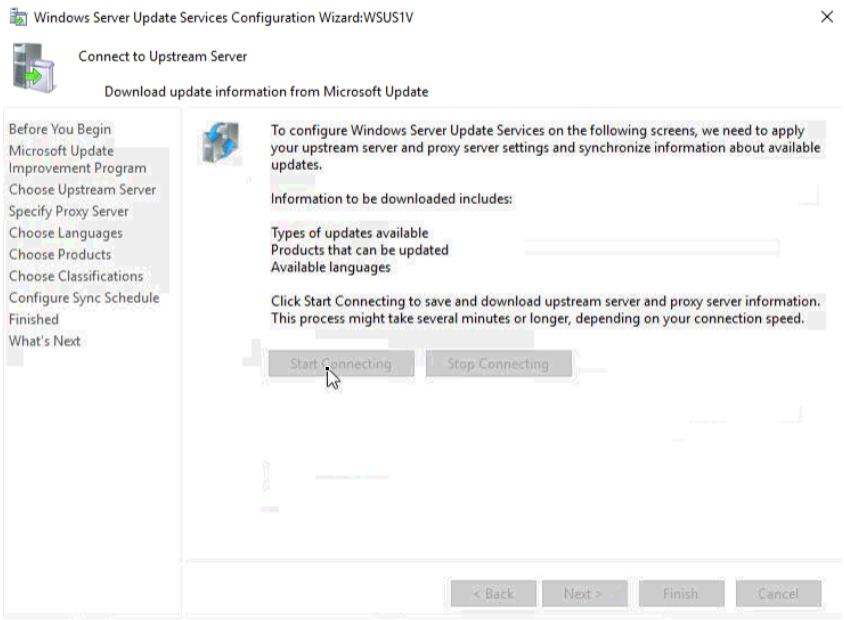
Obrázek 157 - Konfigurace WSUS služby č.2

Na další straně již zvolíme, jestli chceme server synchronizovat s Microsoft Update, nebo budeme synchronizovat server s jiným Windows Update Serverem (v našem případě volíme první možnost).



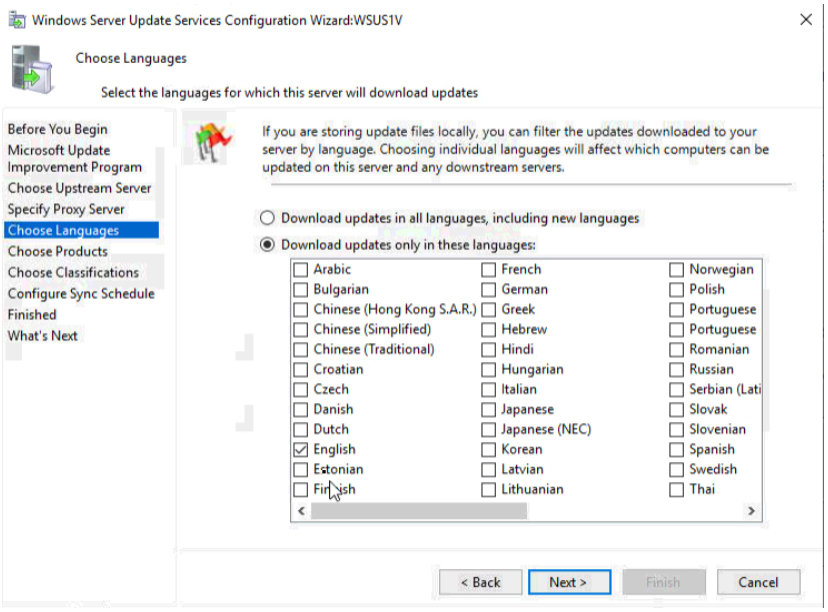
Obrázek 158 - Konfigurace WSUS služby č.3

Další stranu přeskočíme, neboť v rámci infrastruktury nemáme a nebudeme mít zavedený proxy server. Dále se již dostáváme na synchronizační část, kde zvolíme „Start connecting“ a budeme čekat, nežli se server připojí ke službě Microsoft Update.



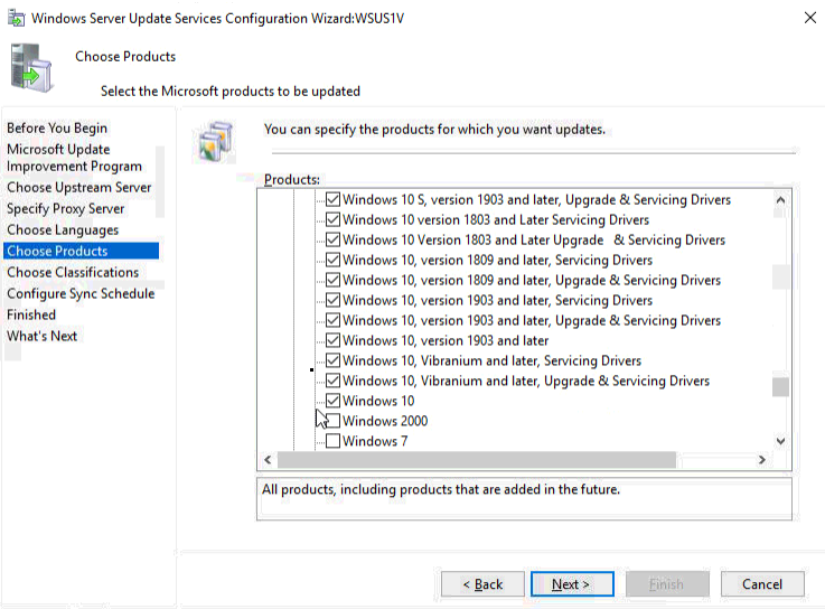
Obrázek 159 - Konfigurace WSUS služby č.4

Připojení může trvat i několik minut, avšak posléze budeme pokračovat a zvolíme na dalším listu jazyk, ve kterém budeme chtít stahovat aktualizace, pro nás zvolíme angličtinu.



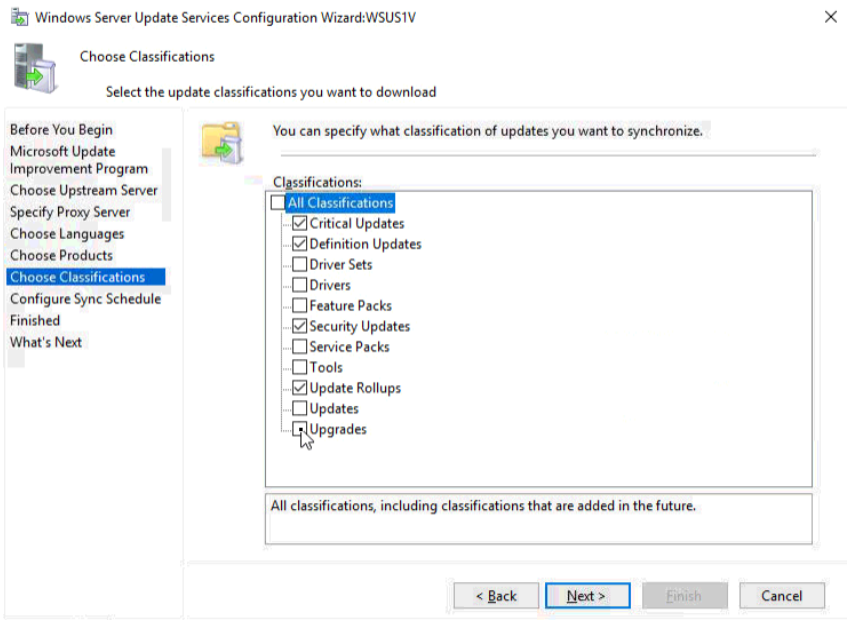
Obrázek 160 - Konfigurace WSUS služby č.5

Na dalším listu následně volíme typy produktů, pro které chceme stahovat aktualizace. Což pro nás budou Windows Server 2019 a Windows 10, všechny ostatní verze můžeme odškrtnout. Samozřejmě později je možné volbu upravit, v případě potřebných změn ve firmě.



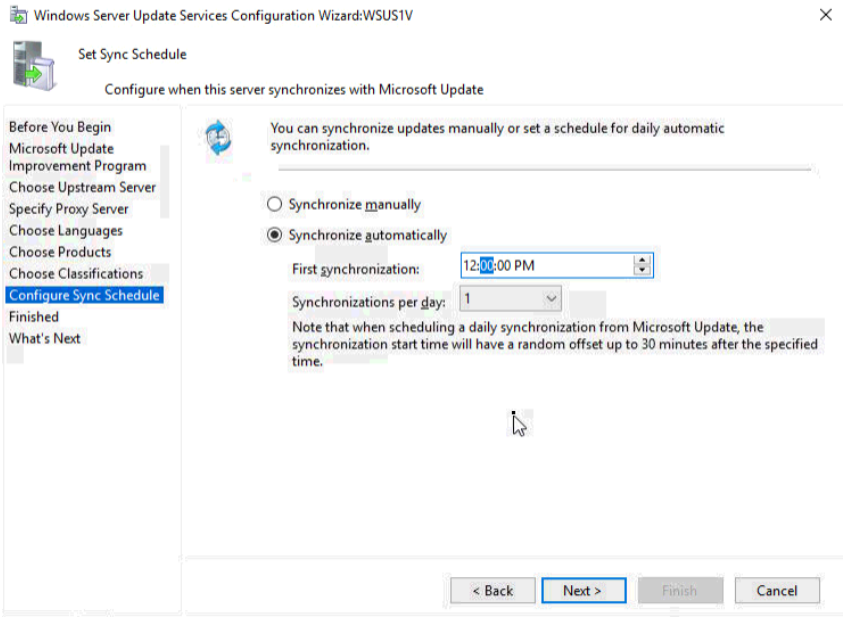
Obrázek 161 - Konfigurace WSUS služby č.6

Další strana nás zavede k výběru typů aktualizací, které budeme stahovat, zde vybereme Kritické aktualizace, Bezpečnostní aktualizace a Rollups, zbytek aktualizovat nechceme pomocí WSUS serveru.



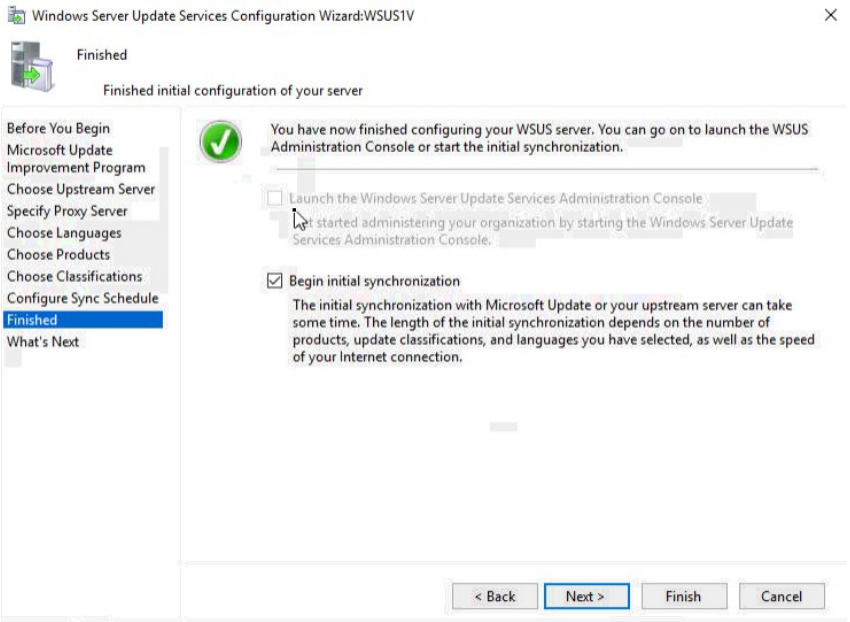
Obrázek 162 - Konfigurace WSUS služby č.7

Následně zvolíme, jestli chceme provádět synchronizaci automaticky, nebo manuálně, kde pro nás bude vhodné zvolit automatickou synchronizaci, neboť tím snížíme počet úkonů, které je nutné dělat manuálně a opakovaně. Nastavíme čas na půlnoc a zvolíme počet synchronizací denně (1).



Obrázek 163 - Konfigurace WSUS služby č.8

Na dalším listu vybereme „Begin initial synchronization“ a pokračujeme, prvotní synchronizace může trvat v řádu minut až desítek minut. Poté dokončíme instalaci serveru.



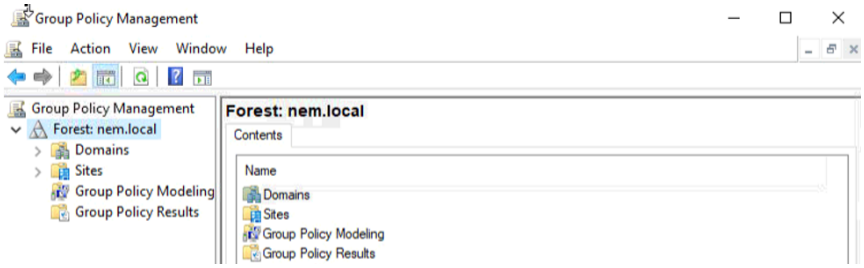
Obrázek 164 - Konfigurace WSUS služby č.9

14.2 Konfigurace politiky pro WSUS

Dalším důležitým úkonem pro funkčnost našeho WSUS serveru bude konfigurace politiky pro automatické aktualizace. Jelikož na klientech (čímž jsou myšleny i server) systém neví, že existuje WSUS server, musíme na něj pomocí zmíněné politiky poukázat.

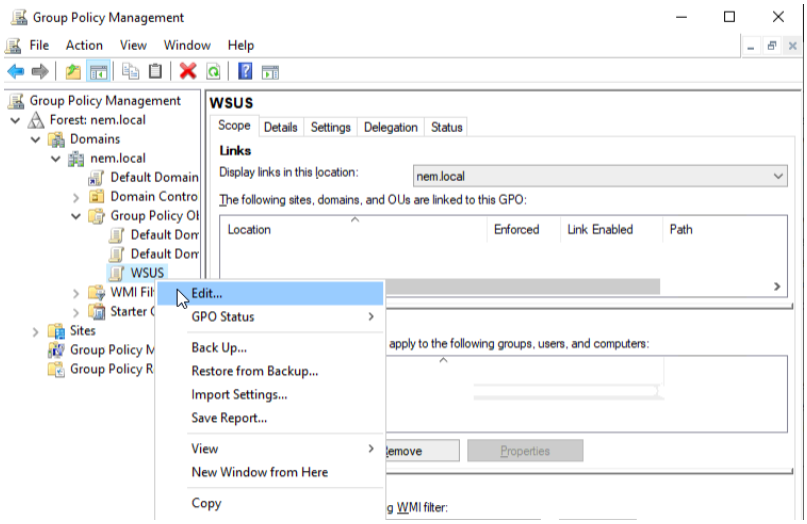
14.2.1 Konfigurace automatických aktualizací WSUS

V rámci Server management na našem DC serveru zvolíme v Tools Group Policy Management, kde následně budeme nastavovat veškeré politiky pro naši infrastrukturu.



Obrázek 165 - Nastavení politiky pro WSUS

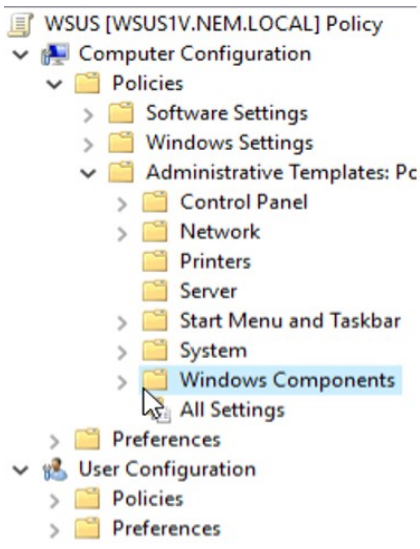
V oddílu Domains/nem.local/Group policy object vytvoříme pomocí pravého tlačítka nový GPO a pojmenujeme jej WSUS. Na náš nově vytvořený objekt WSUS klikneme pravým tlačítkem a zvolíme Edit.



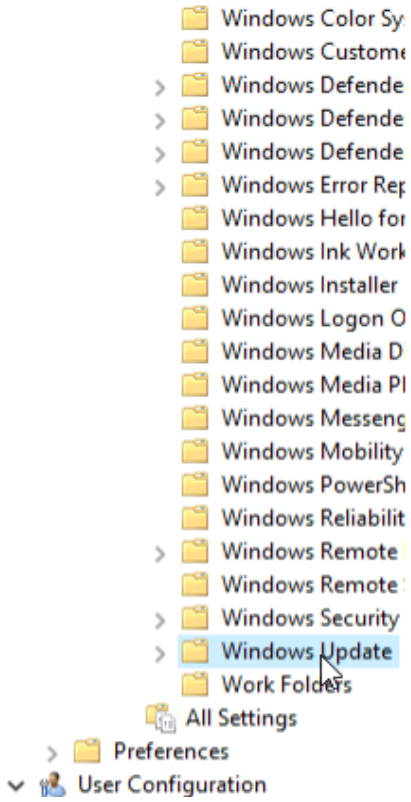
Obrázek 166 - Nastavení politiky pro WSUS č.2

Dále zvolíme v novém okně Computer Configuration poté Policies/Administrative Templates/Windows Components/Windows Update. Kde následně zvolíme Configure

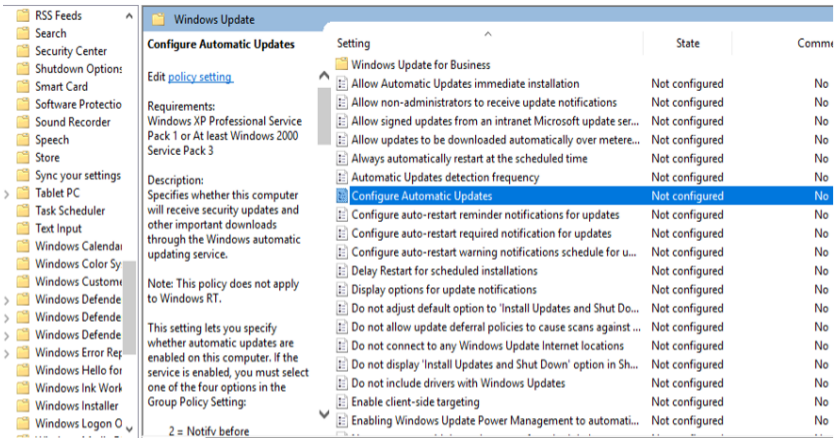
Automatic Updates a tuto politiku povolíme výběrem „Enabled“. Zvolíme zároveň automatické stažení aktualizace a dotaz uživateli, zda je možno instalovat a také den, hodinu, kdy chceme aktualizace aplikovat na klienty.



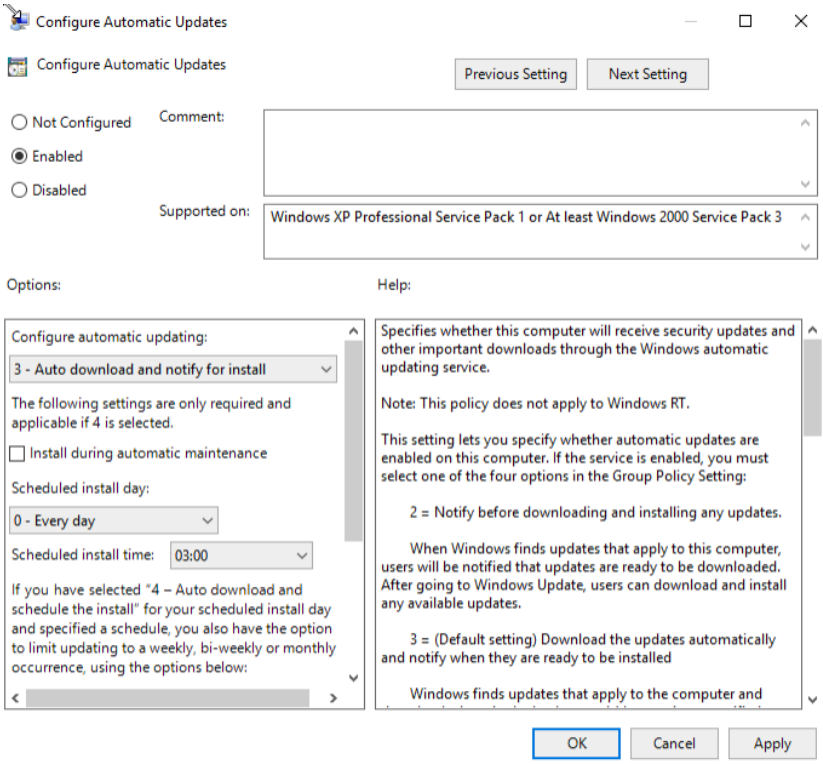
Obrázek 167 - Politiky pro WSUS č.3



Obrázek 168 - Politiky pro WSUS č.4



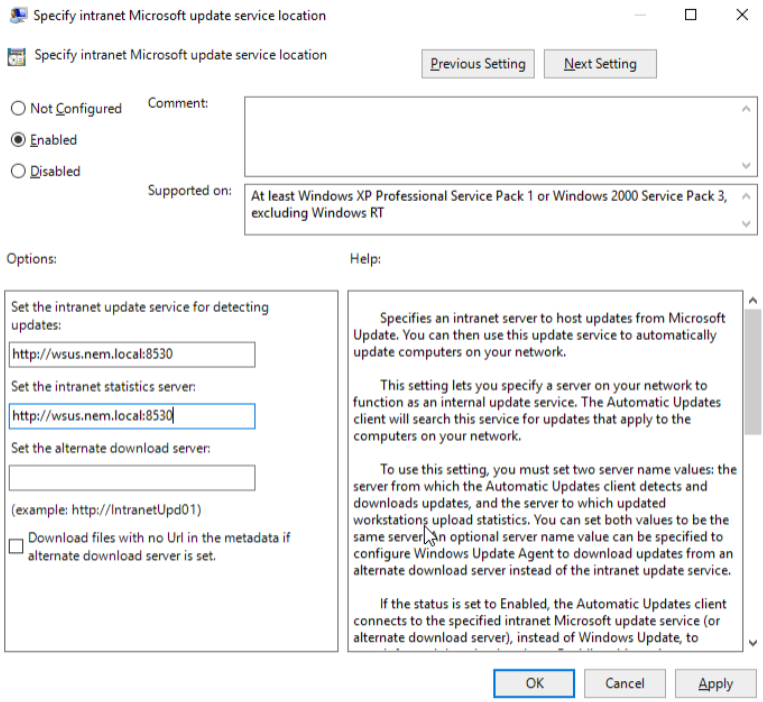
Obrázek 169 - Nastavení politiky pro WSUS č.5



Obrázek 170 - Nastavení politiky pro WSUS č.6

14.2.2 Microsoft Update Service Location

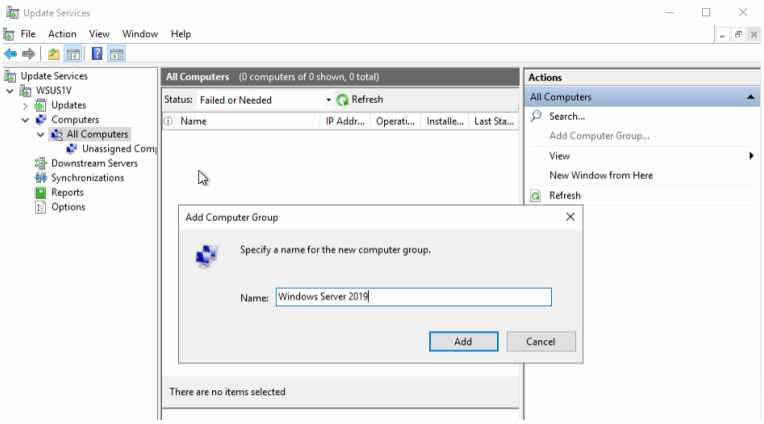
Posléze je potřeba nastavit lokace, odkud se budou na klientech aktualizace stahovat, a to tak, že zvolíme náš lokální server WSUS v rámci doménové politiky, která určí, že klient nebude stahovat aktualizace samostatně z Microsoft Update Serverů, ale pouze z našeho WSUS serveru. Pro toto nastavení otevřeme politiku Specify intranet Microsoft update service location, otevřeme ji a povolíme. Taktéž zde nastavíme zmiňovaný WSUS server a aplikujeme. Windows aktualizace jsou dostupné na portu 8530.



Obrázek 171 - Microsoft Update nastavení lokace

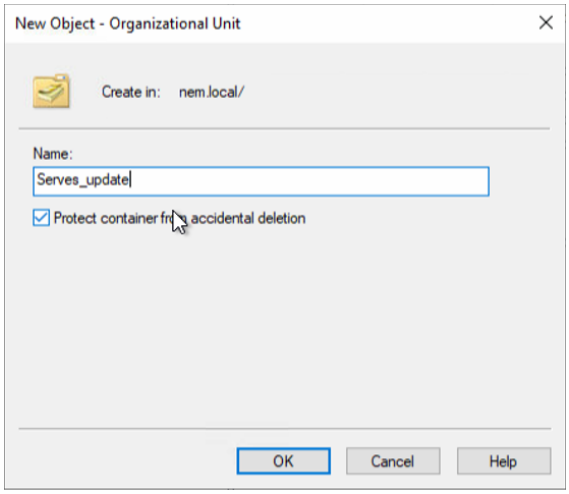
14.3 Vytvoření update skupin a AD konfigurace

Nyní se vrátíme na wsus1v, kde otevřeme Windows Server Update services, kde vybereme WSUS1V/Computers/All Computers, kde pravým tlačítkem vytvoříme nové skupiny (Windows Server 2019 a Windows 10). Nyní máme vytvořené politiky a skupiny pro update serverů, nicméně ještě musíme vytvořit na AD novou skupinu, na kterou se budou dané politiky uplatňovat.



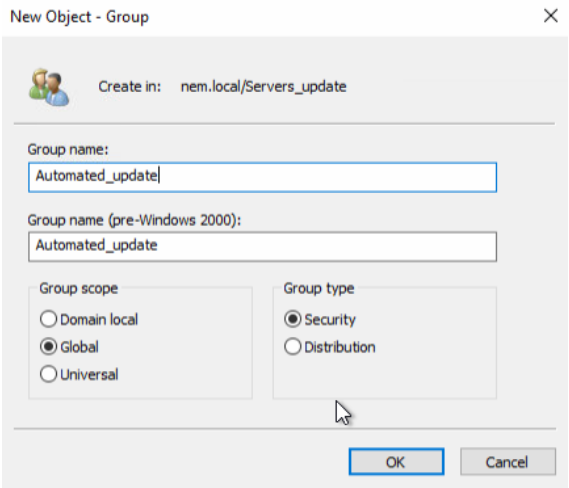
Obrázek 172 - Vytvoření AD skupin

Opětovně se připojíme na náš dc1v server, kde si otevřeme Active Directory Users and Computers. Kde si zvolíme v menu Actions položku New a vytvoříme Organizational Unit. Pojemenujeme ji Server_update a necháme zakliknutou ochranu proti náhodnému odmazání.



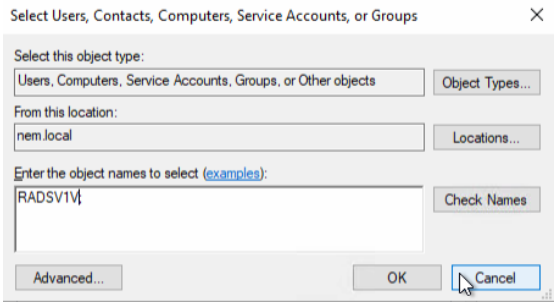
Obrázek 173 - Vytvoření AD skupin č.2

Nyní si do ní přesuneme všechny servery, které máme prozatím v organizační jednotce computers, kam se automaticky vkládají, po připojení do domény. Následně dáme opět Actions a New, kde tentokrát vybereme Group a vytvoříme novou skupinu, na kterou následně budeme aplikovat naši vytvořenou politiku. Pojmenujeme ji Automated_update. Následně vytvoříme ještě organizační jednotku Groups a do ní vytvořenou skupinu přesuneme.



Obrázek 174 - Vytvoření AD skupin č.3

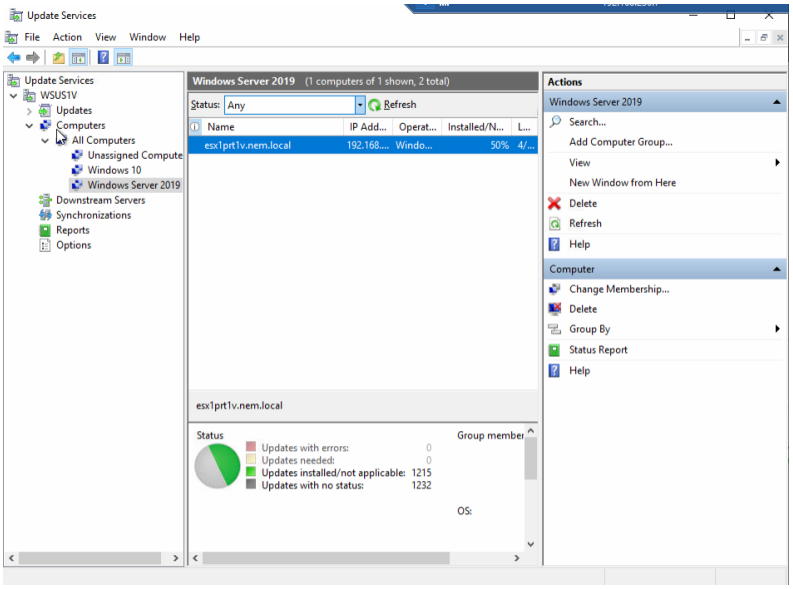
Nyní skupinu rozklikneme a vybereme lištu Members a přidáme všechny naše servery do skupin. Pro přidání vícero objektů naráz používáme středník. Zvolíme Add a zde vypíšeme naše servery (důležité zkontrolovat Object Types, abychom měli zvolený výběr Computers, jinak nám to naše servery nenalezne).



Obrázek 175 - Přidání serverů do skupiny

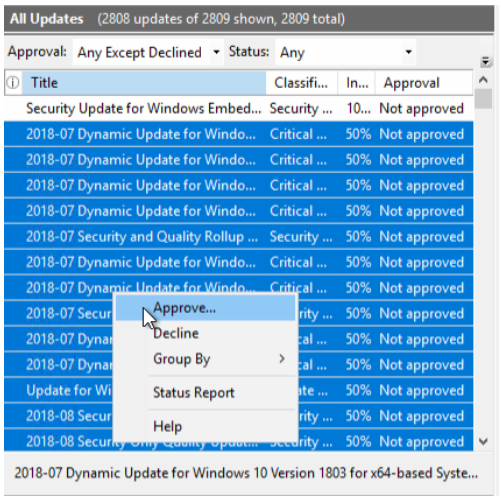
14.4 Aktualizace a možnosti nastavení

Nyní po přidání všech doposud vytvořených serverů a aktualizace jejich politik například restartem se vrátíme zpět na náš WSUS server a v Update Services (zkráceně pro Windows Server Update Services) vybereme All Computers a zde přesuneme do naší vytvořené skupiny všechny doposud připojené servery pomocí pravého kliknutí na daný server a zvolení Change Membership. Nyní jsme schopní v rámci Update Services schvalovat a instalovat pouze ty aktualizace, které chceme.



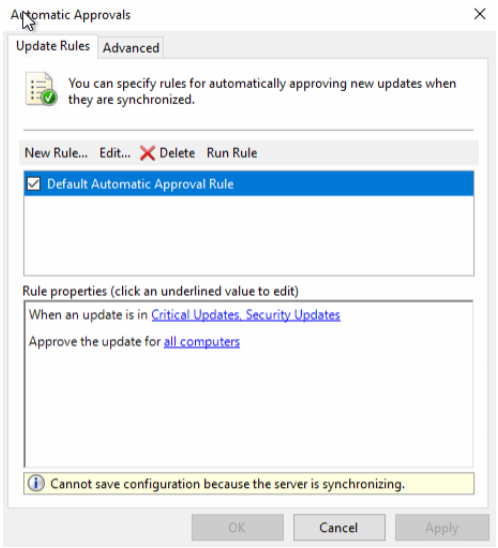
Obrázek 176 - Nastavení Aktualizací

Konkrétně zvolením Updates, kde vybereme All Updates, což nám ukáže všechny dostupné aktualizace. Zde označíme ty, které chceme vpustit na naše počítače a servery v síti a zvolíme pravým tlačítkem Approve. Otevře se nám okno, kde vybereme skupinu, pro kterou bude toto schválení platit.



Obrázek 177 - Schválení aktualizací

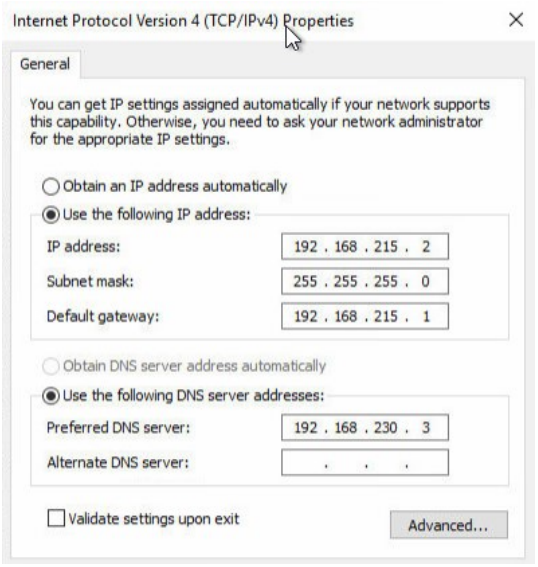
Dále je vhodné nastavit automatická schvalovací pravidla. Otevřeme si Options/Automatic Approvals, kde můžeme vytvořit nové pravidlo pomocí „New rule“. Nicméně my využijeme Default Automatic Approval Rule, které již jen předdefinováno a funguje způsobem, že pokud je aktualizace kritická, je automaticky schválena pro instalaci na všechny počítače/servery. Další důležitou součástí je oddíl Reports. Kde získáme různá data o aplikovaných aktualizacích, počítačích a synchronizacích.



Obrázek 178 - Automatické schvalovací pravidlo

15 INSTALACE BACKUP SERVERU

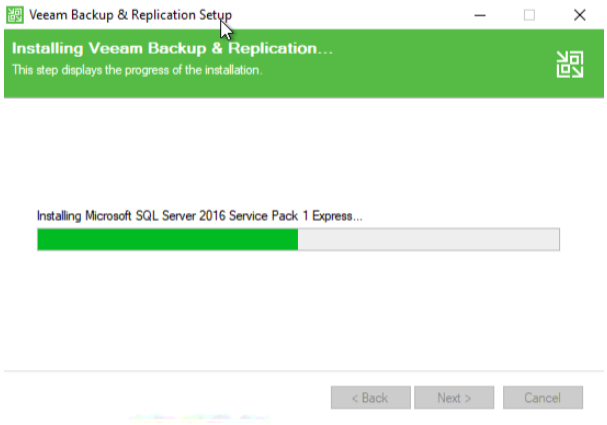
Prvně provedeme stejnou proceduru jako u ostatních Windows serverů. Takže založíme nový VM, kde zvolíme jméno esx1_backupsv1v. Dále zvolíme instalační médium a vybereme síťový port „Backup“. Pro zálohovací server zvolíme větší diskový prostor než u jiných serverů, a to pro důvody záloh všech serverů a možnosti archivace. Konkrétně zvolíme velikost disku 500 GB. Dále pak nainstalujeme Windows Server a provedeme nám již známé základní procedury jako je volba jména serveru (backupsv1v), zadání IP adresy 192.168.215.2, následně přidáme server do domény a poté povolíme RDP. Samozřejmostí je instalace VMtools.



Obrázek 179 - Backup server síťový adaptér

15.1 Instalace a konfigurace zálohovacího softwaru

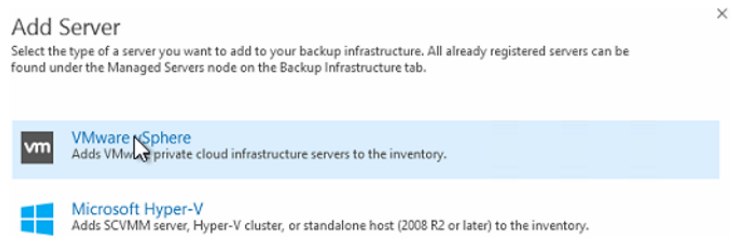
Jak již bylo uvedeno v teoretické části, využijeme zkušební verzi softwaru Veeam, který nám poskytne veškeré podmínky a funkcionality pro zálohu našich serverů. Zároveň umí skvěle pracovat jak s fyzickými servery, či virtuálními ať už na bázi Linuxu, nebo Windows. Je potřeba stáhnout danou zkušební verzi z webu „https://www.veeam.com/cz/data-center-availability-suite.html“. Následně nainstalujeme, kde v rámci instalace si software doinstaluje chybějící funkcionality systému, jako jsou SQL server, Powershell 2.0 a další. Instalace trvá velmi dlouho, neboť obsahuje velké množství různých utilit a dalších funkcí.



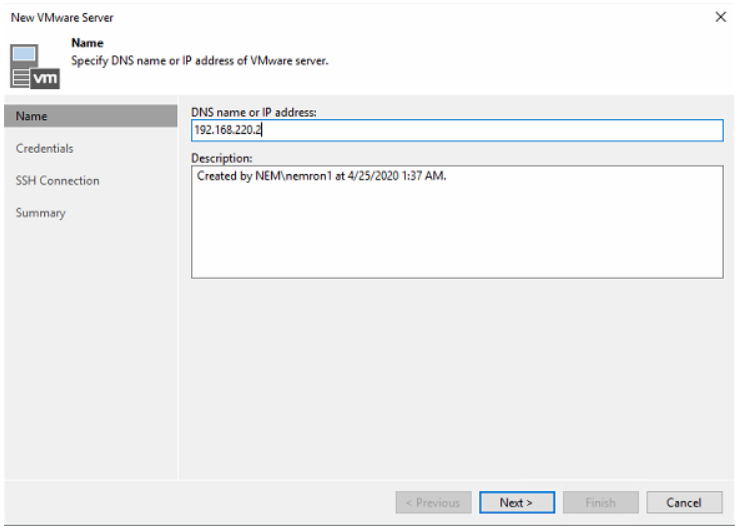
Obrázek 180 - Instalace Veeamu

15.2 Konfigurace Veeamu

Po dokončení instalace zavedeme náš VMware host do databáze Veeamu abychom byli schopni z něj zálohovat. Po otevření Veeam konzole zaklikneme Inventory a přidáme nový virtuální server. Na otevřené stránce zvolíme VMware Vsphere. Dále zadáme DNS jméno nebo IP adresu našeho ESXi hosta. Na další straně přidáme přihlašovací údaje pro hosta a dokončíme přidání. [19]

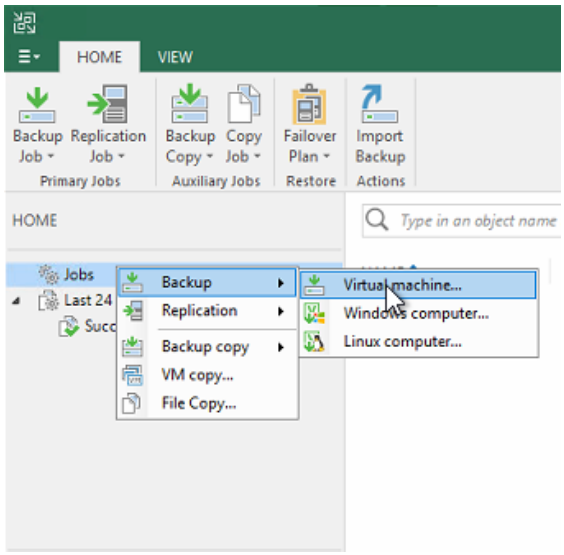


Obrázek 181 - Konfigurace Veeamu



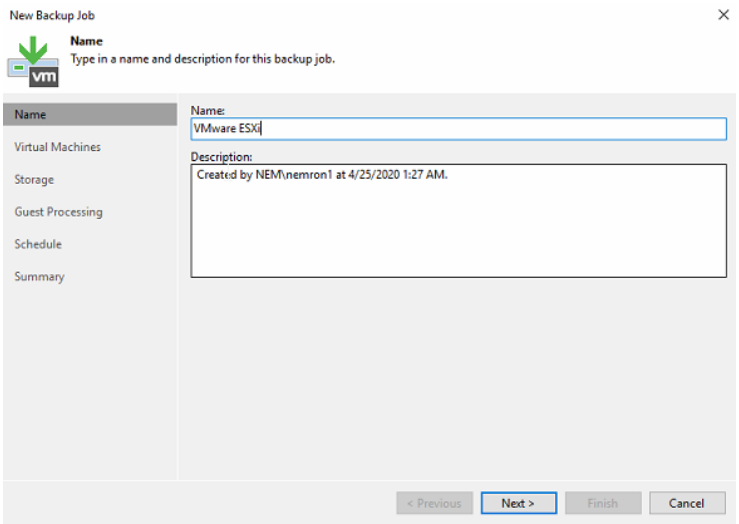
Obrázek 182 - Konfigurace Veeamu č.2

Následně pak otevřeme lištu Home a pravým tlačítkem zvolíme „Jobs“, kde následně vybereme Backup a Virtual Machine.



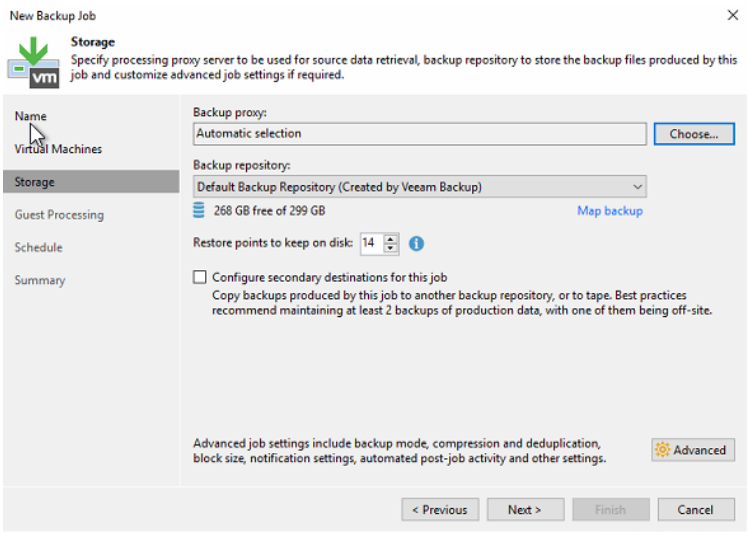
Obrázek 183 - Konfigurace Veeamu č.3

Otevře se okno nové zálohovací úlohy, tu je potřeba pojmenovat (pro nás VMware ESXi) a následně na dalším listu zvolíme virtuální stroje, které chceme přidat. Zvolíme Add a přidáme všechny naše servery kromě fs1v, který budeme chtít zálohovat v jiné časové frekvenci. [19]

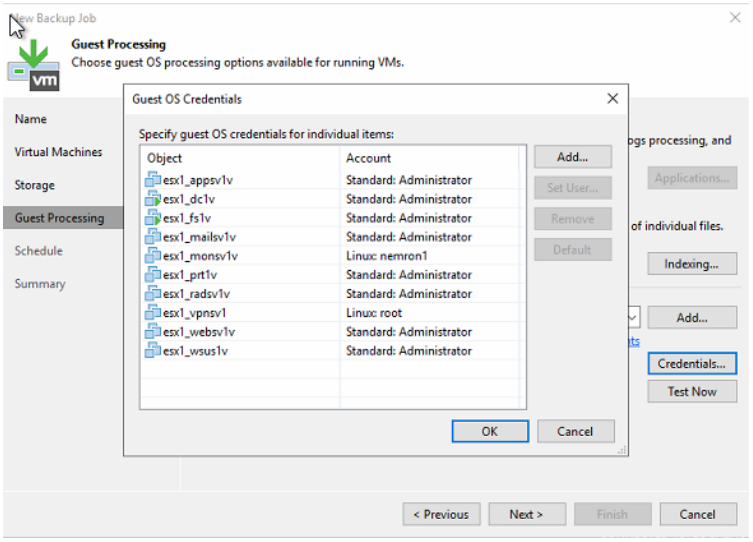


Obrázek 184 - Konfigurace Veeamu č.4

Na dalším listu pokračujeme definováním místa pro uložení zálohy. Na dalším listu následně přiřadíme přihlašovací údaje jednotlivým serverům. A povolíme indexování zálohovaných dat, pro rychlejší a jednodušší obnovu, v případě ztráty jednotlivých souborů či složek. [19]

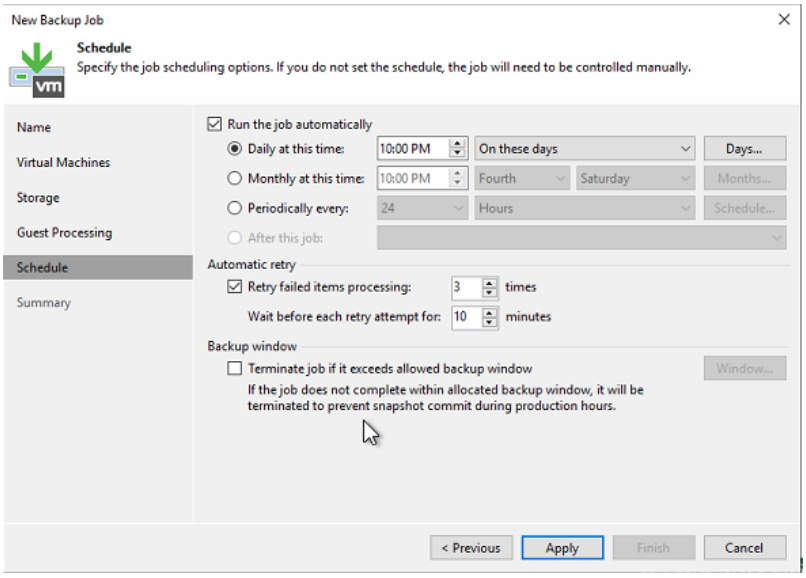


Obrázek 185 - Konfigurace Veeamu č.4



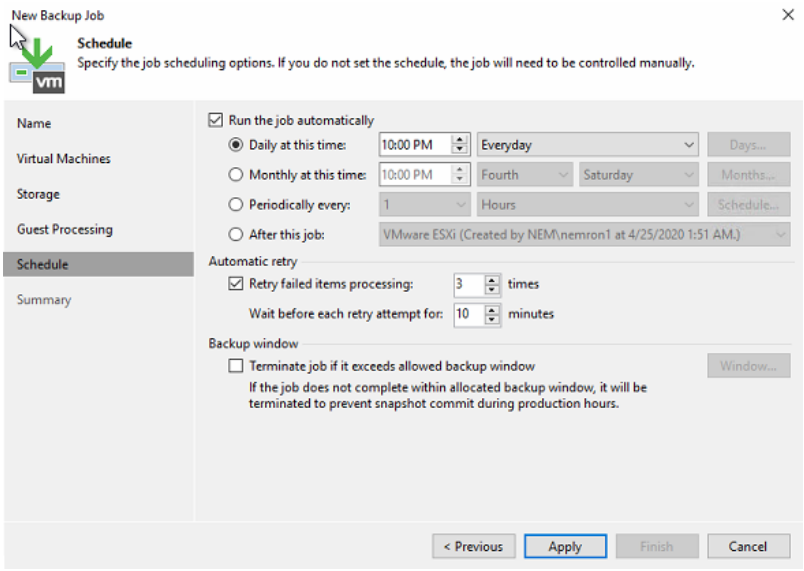
Obrázek 186 - Konfigurace Veeamu č.5

Na dalším listu pak zvolíme, že se bude záloha opakovat každý týden v neděli ve 22:00 a zároveň při nezdařeném pokusu se bude pokoušet o obnovu zálohování 3 minuty po neúspěšném pokusu. Poté zvolíme Apply a dokončíme.



Obrázek 187 - Konfigurace Veeamu č.6

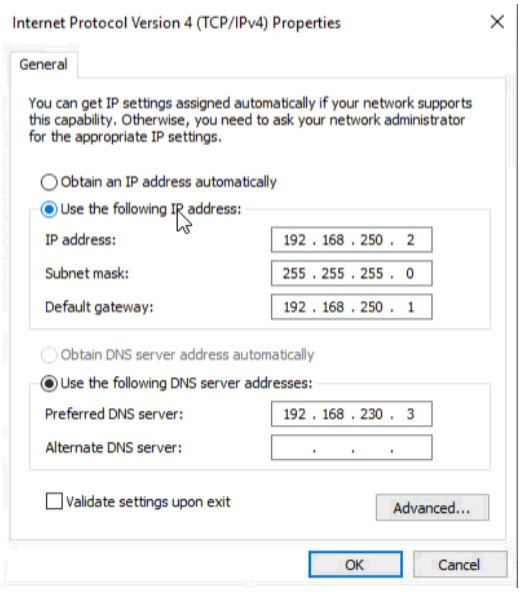
Nyní vytvoříme druhou úlohu stejným způsobem, kde jméno zvolíme VMware_fileserver, mezi zálohované servery přidáme pouze fs1v, určíme zálohu probíhající denně v 22:00 a zvolíme Apply.



Obrázek 188 - Konfigurace Veeamu č.7

16 INSTALACE WEBOVÉHO SERVERU

Webový server nainstalujeme jako ostatní servery s operačním systémem Windows. Připravíme virtuální stroj (esx1_websv1v) přiřazený do port skupiny Servers. Systém nainstalujeme, přiřadíme mu statickou IP adresu (192.168.250.2), přejmenujeme (websv1v), přidáme do domény, povolíme RDP a nainstalujeme VMtools. Nyní je náš server připraven na konfiguraci.

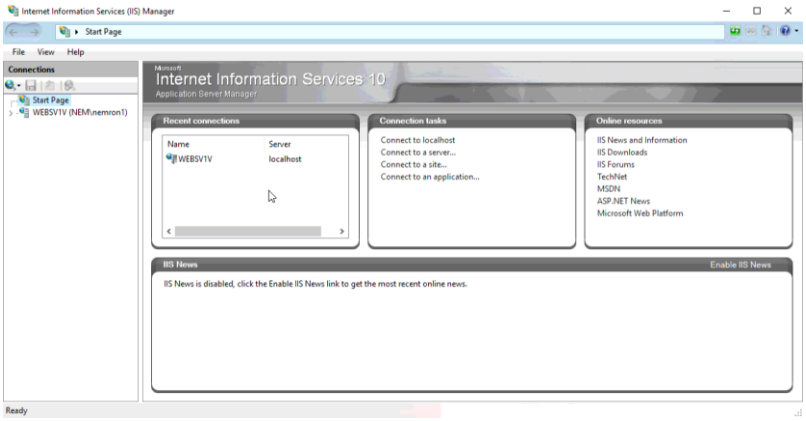


Obrázek 189 - Web server síťový adaptér

Dále v Server Manageru přidáme další funkce a možnosti, zvolíme náš server, na další stránce vybereme Web Server (IIS). Budeme dotázání, zda chceme nainstalovat dané funkce. Dále již jen dokončíme instalaci.

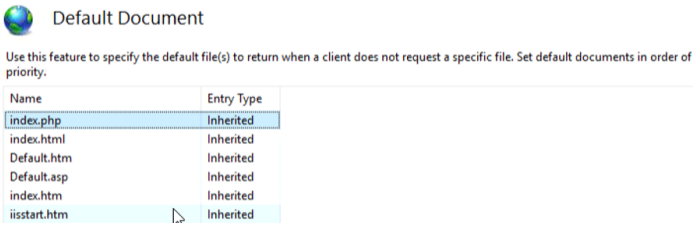
16.1 Konfigurace defaultní webové stránky

Po instalaci samotného Web Serveru musíme ještě nakonfigurovat první stránku, pro kterou následně použijeme volně dostupnou webovou šablonu z internetu. Pro konfiguraci si otevřeme Server Manager/Tools/Internet Information Services (IIS) Manager.

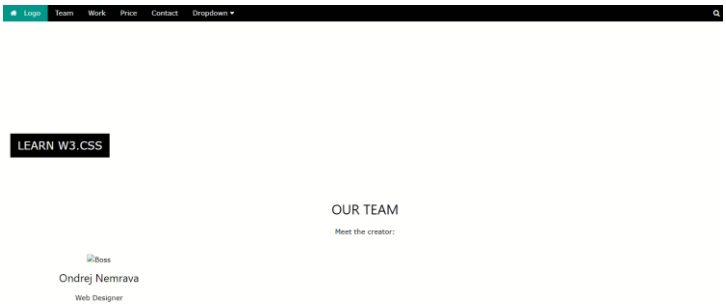


Obrázek 190 - IIS menu

Rozevřeme nabídku našeho serveru, kde si zvolíme Sites a následně Default Site. Nyní je potřeba vytvořit zkušební stránku, kterou otestujeme a nastavíme. Na webu stáhneme dostupnou šablonu z webu w3schools, kterou vložíme do již vytvořené složky inetpub/wwwroot na disku C: našeho serveru jako index.php. V rámci IIS Manageru vybereme položku Default Document, kde posuneme náš vytvořený index.php, až na vrchol listu pro lepší responzivitu systému. Nyní si můžeme zobrazit naši intranetovou webovou stránku. [24]



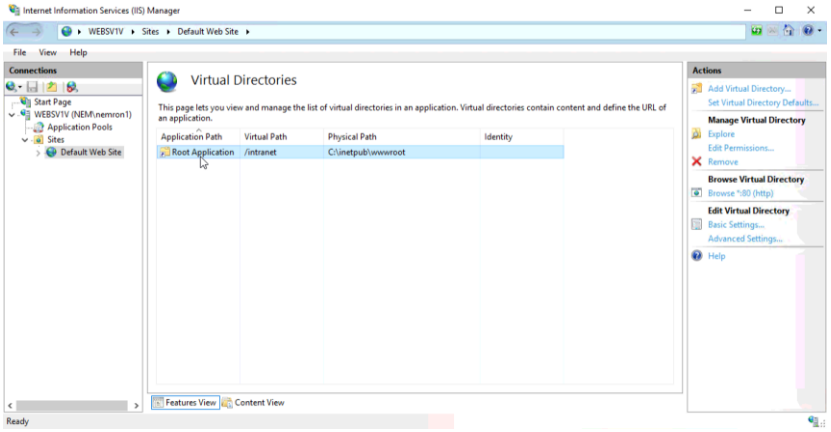
Obrázek 191 - IIS defaultní dokument



Obrázek 192 - Webová stránka

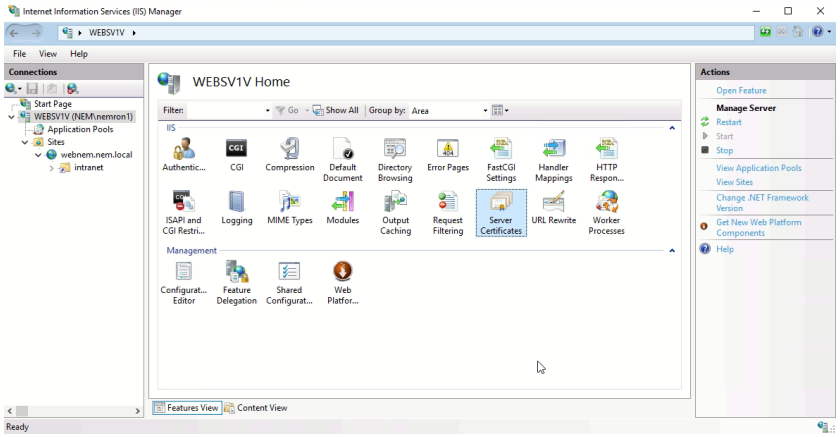
16.2 Konfigurace virtuálního adresáře

V menu IIS si vybereme View Virtual Directories, zde zvolíme Add Virtual Directory. V novém okně vybereme název (pro nás intranet), a cestu ke složce, na kterou budeme odkazovat.

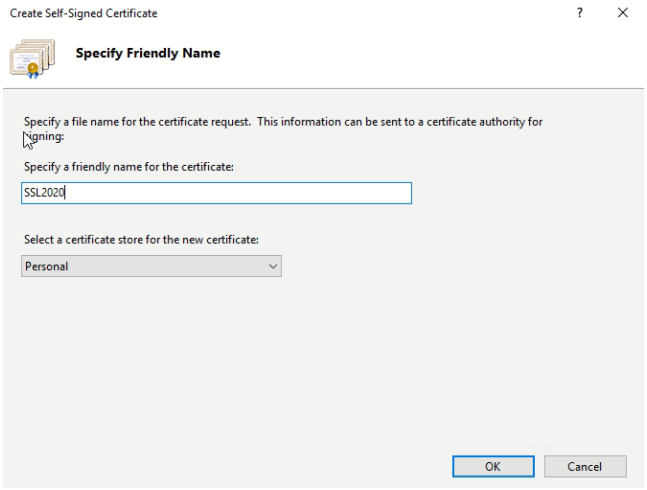


Obrázek 193 - Konfigurace virtuálního adresáře

Nyní když se budeme chtít připojit na intranet, již stačí pouze zvolit IP adresu serveru a název našeho nově vytvořeného virtuálního adresáře (192.168.250.2/intranet). Nicméně pro plnou funkčnost si ještě vytvoříme Selfhosted SSL certifikát a přidáme webu DNS záznamy. Zvolíme Server Certificates a poté v pravém menu Create Self-signed certificate. V následujícím okně pak vytvoříme název a zvolíme Personal.

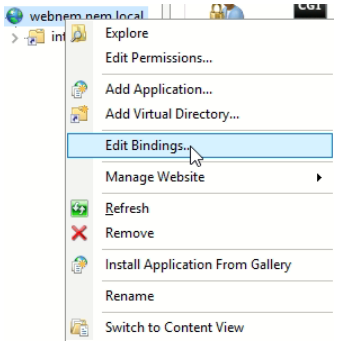


Obrázek 194 - Certifikáty



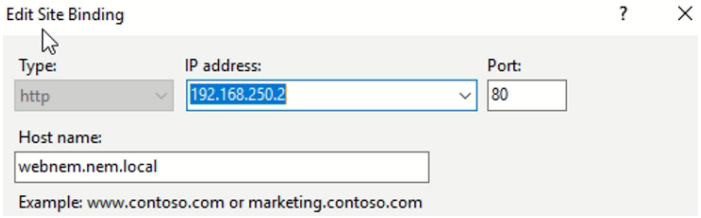
Obrázek 195 - Vytvoření certifikátu

Poté pravým tlačítkem zvolíme naši defaultní stránku a vybereme Edit Bindings.

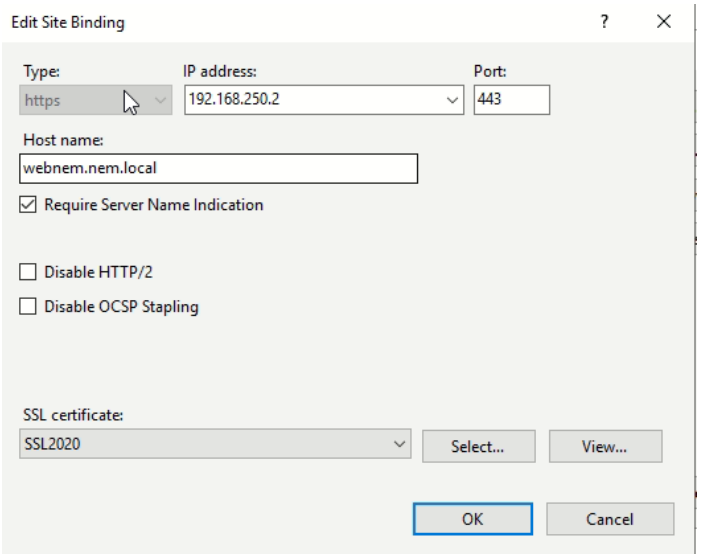


Obrázek 196 - Nastavení spojení

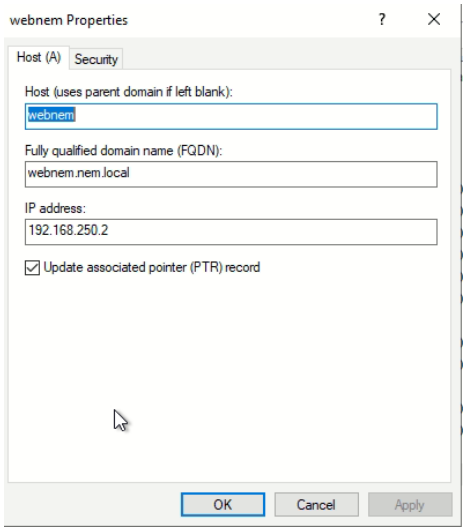
Nejprve vytvoříme spojení pro http a posléze pro https (kde zvolíme náš nově vytvořený certifikát. Dále na našem DNS serveru přidáme záznam, abychom byli schopni přeložit IP adresu 192.168.250.2 na webnem.nem.local.



Obrázek 197 - Nastavení spojení č.2



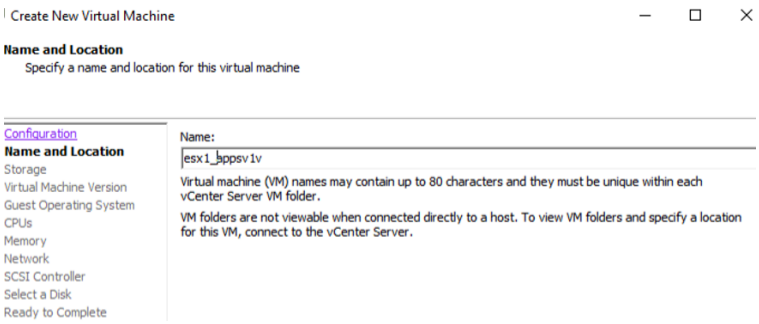
Obrázek 198 - Nastavení spojení č.3



Obrázek 199 - Nastavení spojení č.4

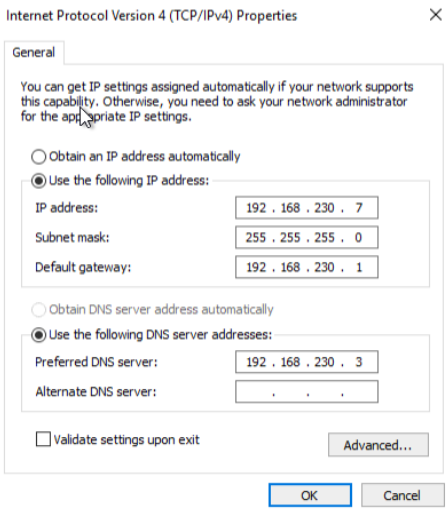
17 INSTALACE APLIKAČNÍHO SERVERU

U instalace aplikačního serveru budeme prakticky postupovat identicky, neboť aplikační server je taktéž Windows Server 2019. Připravíme si virtuální stroj, volíme název VM (esx1_appsv1v).



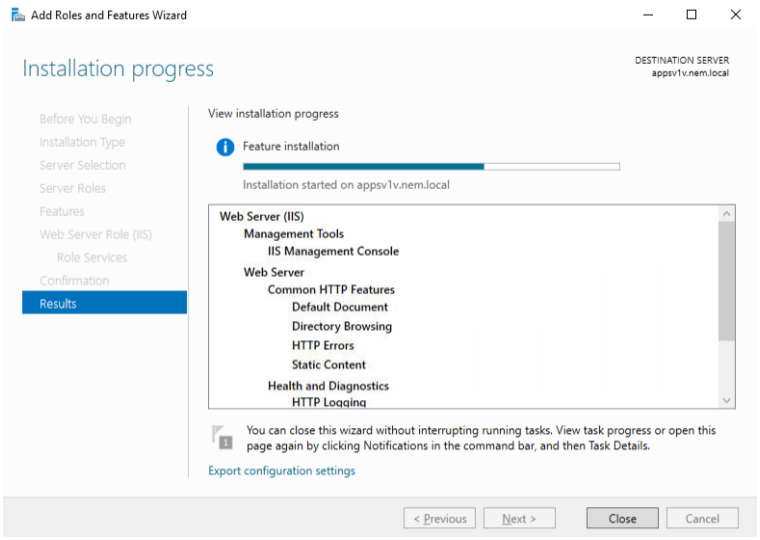
Obrázek 200 - Vytvoření appsv1v VM

Vybereme verzi operačního systému pro náš nový VM. Následně zvolíme standartní úložiště a přidáme server do portu Servers. Zvolíme 1 procesorové jádro a 2 GB RAM. Následně nainstalujeme již klasicky Windows server, zvolíme jméno (appsv1v), povolíme RDP, přiřadíme statickou IP adresu (192.168.230.7), nainstalujeme VMtools a následně přidáme server do naší domény.



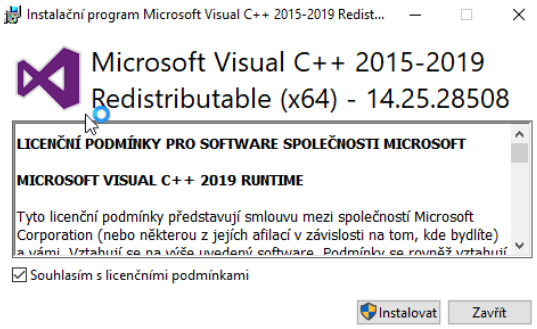
Obrázek 201- Aplikační server síťový adaptér

Po restartu serveru nainstalujeme, stejně jako u Webového serveru, který jsme instalovali v kapitole 15., přidáme IIS služby a funkce pomocí Server Manageru.



Obrázek 202 - Konfigurace aplikačního serveru

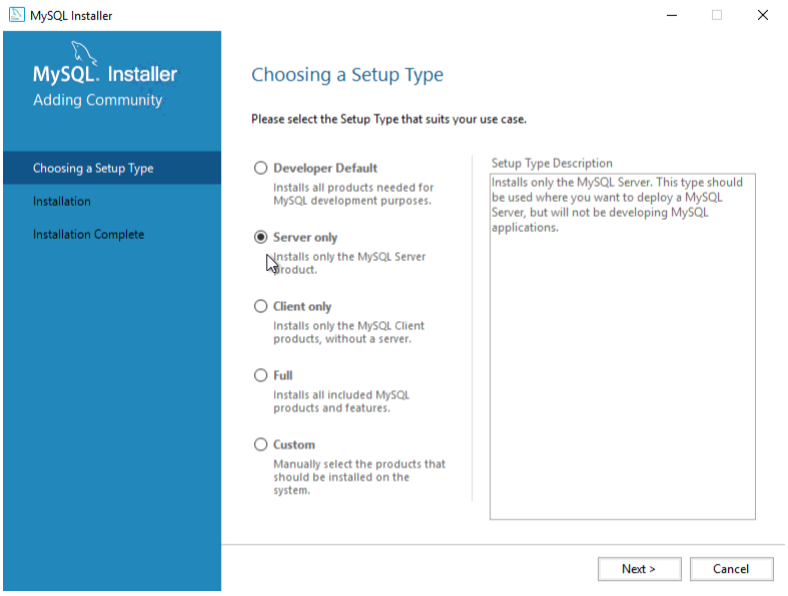
Po restartování systému je nejprve potřeba na server dohrát C++ knihovny od Microsoftu, které máme již nahrané na náš File-server, a proto stačí pouze spustit stažené soubory ze sharu (192.168.230.20/e). Je potřeba nainstalovat obě verze, a to 32bit a 64bit.



Obrázek 203 - Instalace C++

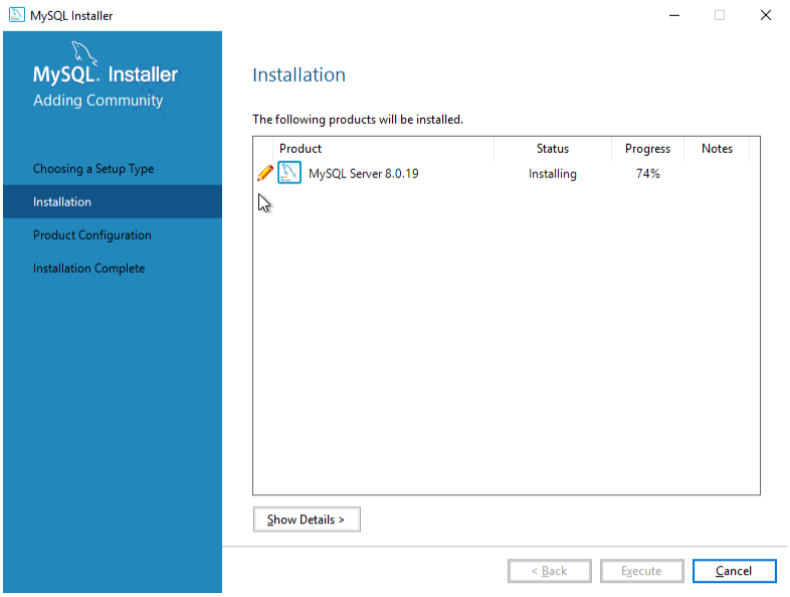
17.1 Instalace mySQL serveru

Nyní je potřeba nainstalovat MySQL server. Prvně je nutné si daný soubor stáhnout z webové stránky MySQL „https://dev.mysql.com/downloads/file/?id=492815“. Následně instalaci spustíme.



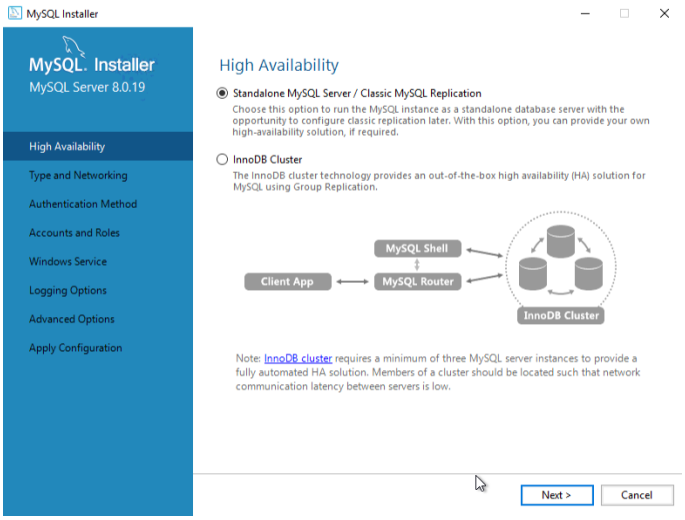
Obrázek 204 - MySQL instalace

Na prvním listu průvodce zvolíme instalaci pouze pro server. Následně na další straně spustíme instalaci.

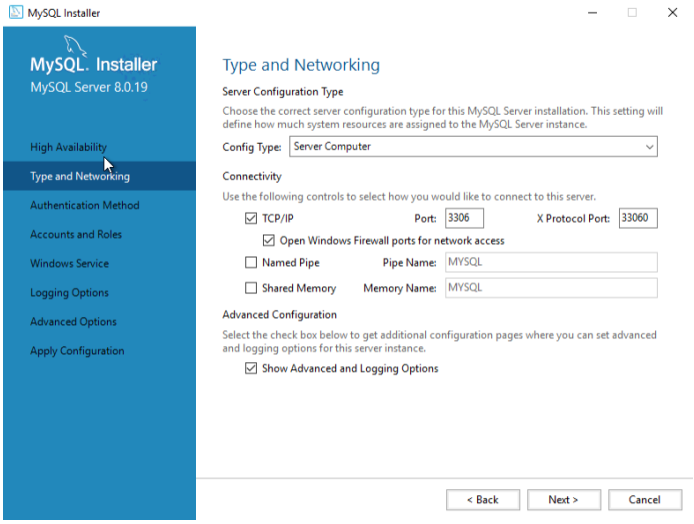


Obrázek 205 - MySQL instalace č.2

Dále pak vybereme Standalone MySQL Server a poté vybereme konfiguraci pro Server (Server Computer), zbytek nastavení nechám v defaultu.

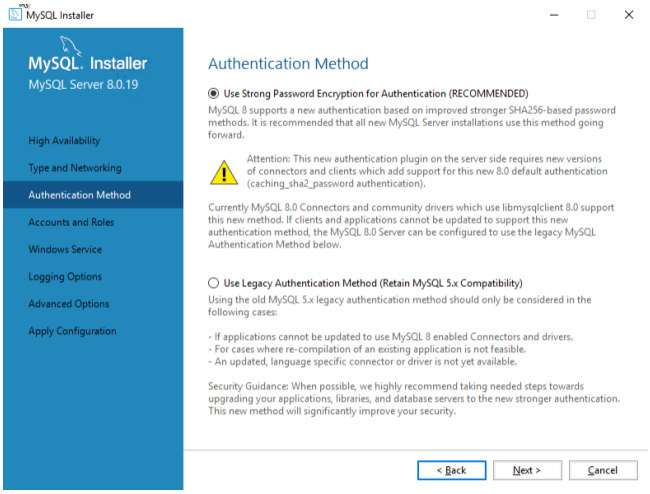


Obrázek 206 - MySQL instalace č.3



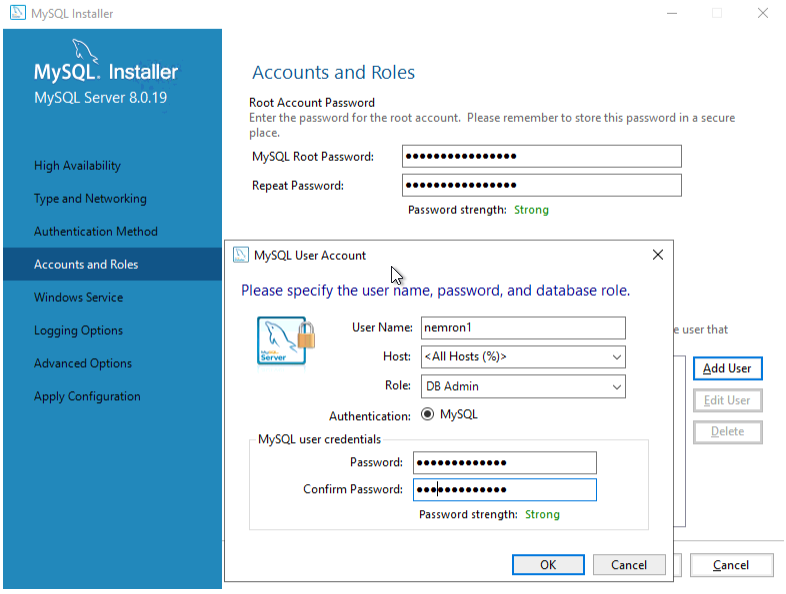
Obrázek 207 - MySQL instalace č.4

Na další straně zvolíme metodu ověření a zvolíme Strong Password Encryption pro vyšší ochranu.



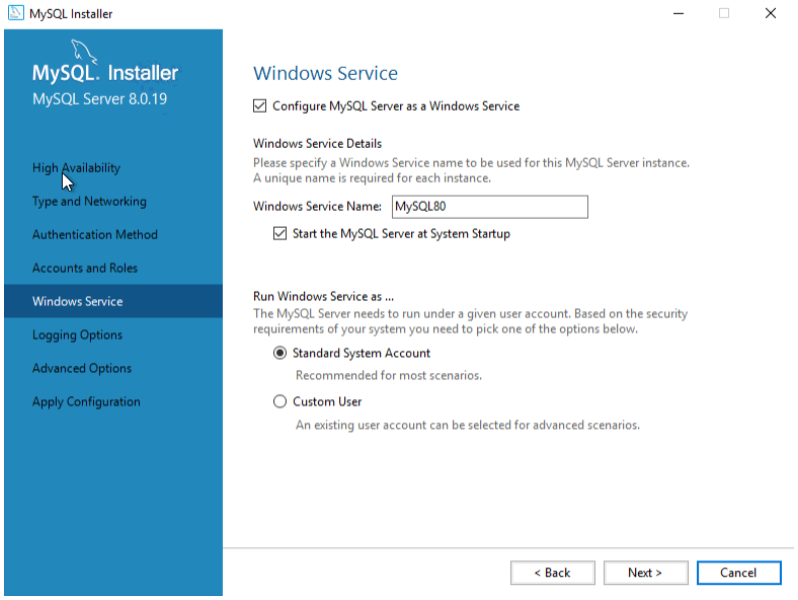
Obrázek 208 - MySQL instalace č.5

Na další straně následně zvolíme heslo pro uživatele root, samozřejmě co nejsilnější, které si budeme schopni zapamatovat a vytvoříme nového uživatele pro administraci databází, taktéž se silným heslem (pro nás uživatel nemron1).

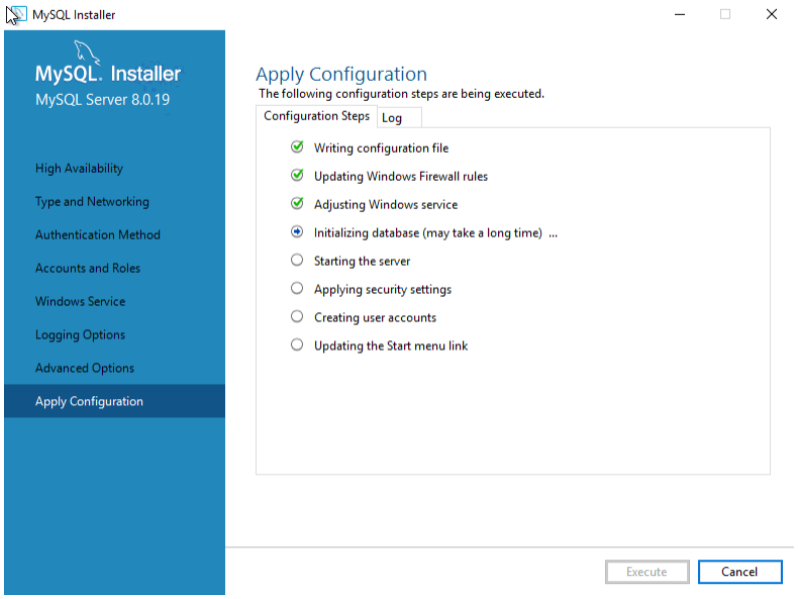


Obrázek 209 - MySQL instalace č.6

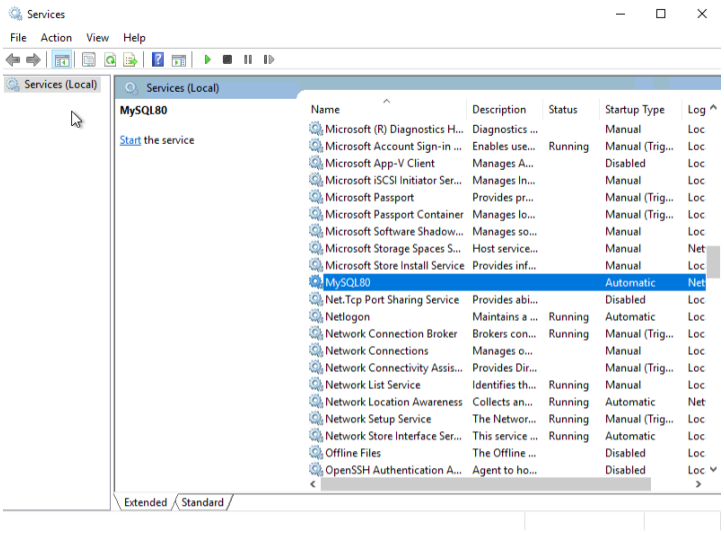
V následujícím kroku zvolíme konfiguraci MySQL serveru jako Windows službu. Následující strana je pouze pro konfiguraci logů a jejich ukládání, což necháme tak jak je a posuneme se dále a stejně tak další stranu nebudeme měnit.



Obrázek 210 - MySQL instalace č.7



Obrázek 211 - MySQL instalace č.8

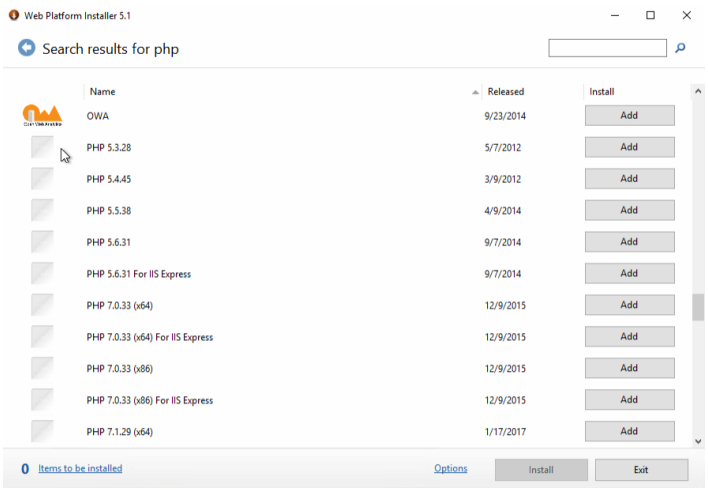


Obrázek 212 - MySQL služba

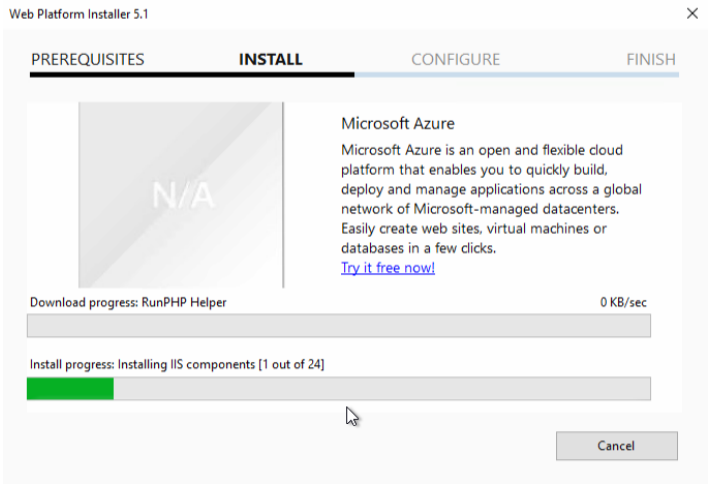
17.2 Instalace rozšíření IIS

Nyní stáhneme rozšíření pro náš IIS server konkrétně Web Platform Installer (dostupný z webu („https://www.microsoft.com/web/downloads/platform.aspx“). A poté ještě stáhneme další rozšíření, a to PHP Manager (dostupný z webu „https://www.iis.net/downloads/community/2018/05/php-manager-150-for-iis-10“).

Následně oba doplňky nainstalujeme. Nyní si otevřeme Web Platform Manager a nainstalujeme si potřebné verze PHP pro osTicket. To budou verze (primárně 7.3, nicméně přidáme i starší a novější pro budoucí případné úpravy a kompatibilitu). Po vybrání PHP verzí, potvrdíme instalaci.

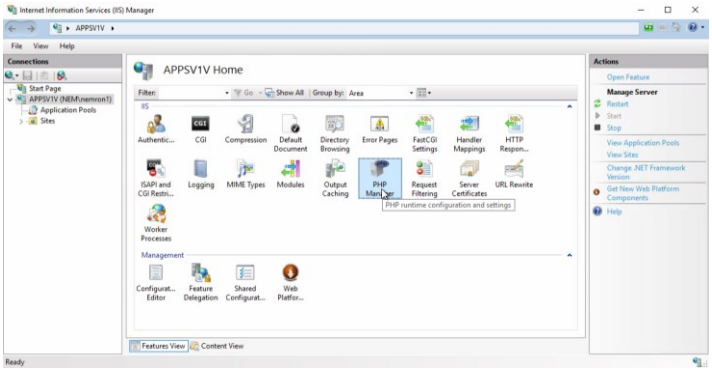


Obrázek 213 - Instalace IIS rozšíření



Obrázek 214 - Instalace IIS rozšíření č.2

Nyní otevřeme Server Manager/Tools a vybereme IIS, kde si zvolíme náš server, a objeví se nabídka, ve které otevřeme PHP Manager.

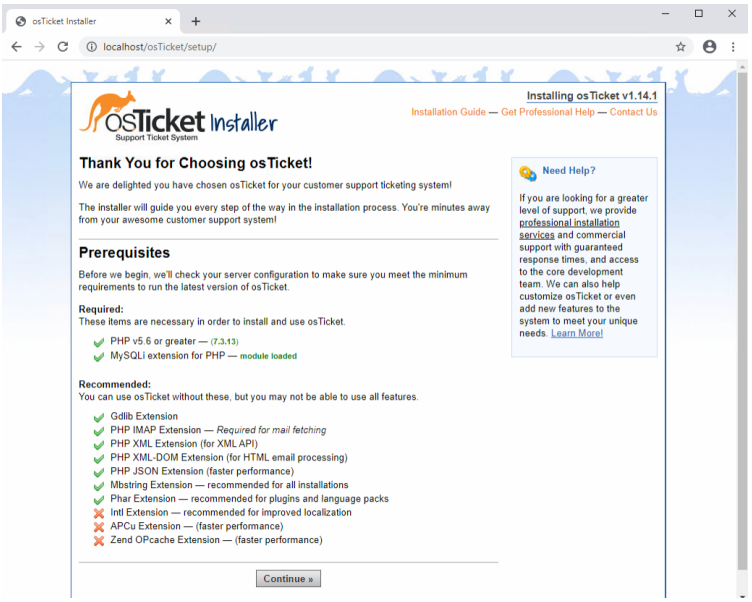


Obrázek 215 - PHP manager

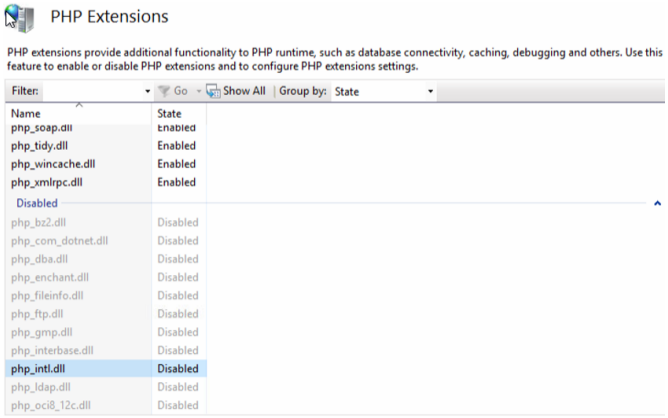
Kde pomocí Change PHP version, zvolíme doporučenou verzi pro osTicket, což je verze 7.3. Po dokončení instalací, si můžeme z webu osTicket stáhnout poslední verzi ticketovacího systému osTicket („https://osticket.com/editions/“). V rámci stahování souboru můžeme vybrat jazyky, které budou dostupné (čeština, angličtina) a dodatečné moduly (pro nás LDAP authentification). Po stažení souboru, extrahujeme data do naší připravené složky „C:\inetpub\wwwroot\osTicket\“. Následně poté překopírujeme stažený soubor LDAP doplňku do podsložky \include\plugin abychom jej posléze mohli nainstalovat. [20]

17.3 Instalace osTicket systému

Následně je potřeba si otevřít prohlížet a zadat URL adresu „localhost/osticket“, což nám otevře instalačního průvodce pro osTicket. Jak vidíme na první stránce, chybí nám některé důležité rozšíření PHP, a proto je pomocí IIS a následně PHP Manageru přidáme tak, že v PHP Manageru zvolíme Enable or Disable Extensions, kde vybereme php_intl.dll a pravým tlačítkem zvolíme Enable. Dále ještě přidáme php_ldap. Nyní zvolíme v prohlížeči continue. Následujícím krokem je vytvoření konfiguračního souboru pro náš systém, nejprve musíme zkopírovat soubor „ost-sampleconfig.php“, který se nachází v „C:\inetpub\wwwroot\osTicket\include“ následně zkopírovaný soubor přejmenujeme na ost-config.php a je potřeba na něm nastavit práva pro přístup osTicket systému, neboť bude potřebovat soubor upravovat. Nyní si v prohlížeči pomocí continue zobrazíme další stránku, kde již provedeme základní nastavení osTicket webového systému. [20]

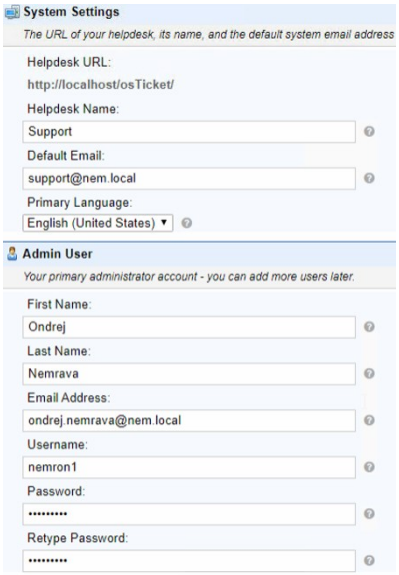


Obrázek 216 - Instalace osTicket



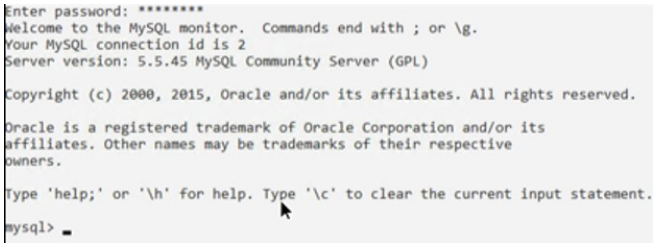
Obrázek 217 - PHP rozšíření

Vyplníme jméno systému (Support), doplníme odpovídající email (support@nem.local), následně vytvoříme prvního administrátora (což doplníme stejně jako je tento uživatel v Active Directory). Dále si musíme vytvořit databázi v mySQL pro náš systém. Otevřeme si mySQL Command Line Client a přihlásíme se pomocí dříve zvoleného hesla pro účet root. [20]



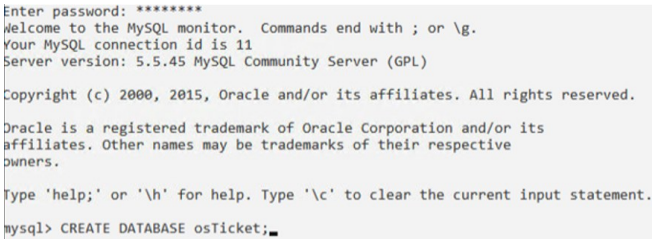
Obrázek 218 - Vytvoření účtu administrátora

17.4 Vytvoření mySQL databáze



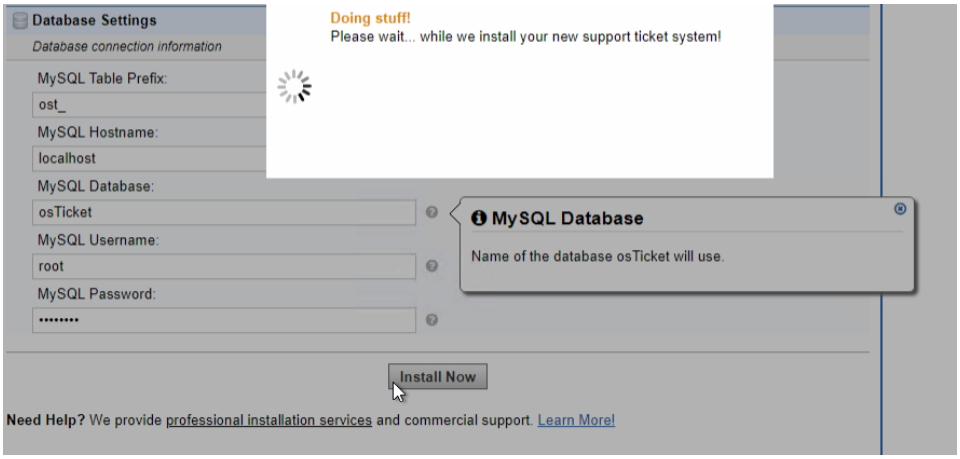
Obrázek 219 - Vytvoření MySQL databáze

Následně vytvoříme novou databázi (osTicket) pomocí query „CREATE DATABASE osTicket;“.



Obrázek 220 - Vytvoření MySQL databáze č.2

Nyní můžeme pokračovat instalaci v prohlížeči, doplníme informace, kde MySQL Hostname bude localhost, MySQL Database bude osTicket a MySQL Username bude root se zvoleným heslem, následně pokračujeme zvolením Install Now.



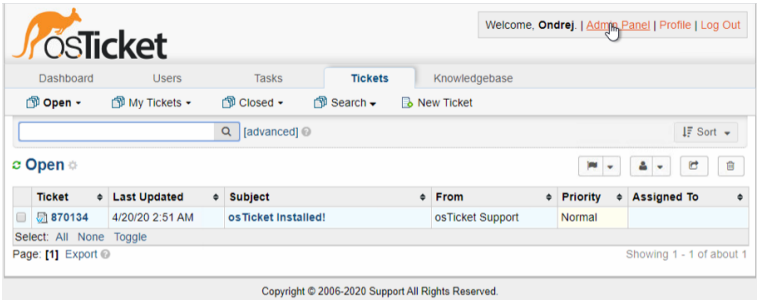
Obrázek 221- Konfigurace databáze

Po dokončení instalace můžeme opětovně odebrat práva na zápis do konfiguračního souboru. Nyní se opětovně podíváme na „http://localhost/osTicket/scp/login.php“, kde se přihlásíme pomocí našeho zvoleného uživatelského jména a hesla.

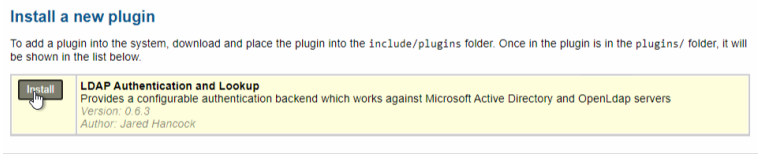
17.5 Konfigurace osTicket

Obrázek 222 - Konfigurace osTicket

Na další obrazovce zvolíme Admin panel, kde následně vybereme možnost Manage/Plugins, kde posléze vybereme Add New plugin a nainstalujeme LDAP Authentication and Lookup plugin. Po přidání doplňku je nutné jej nastavit. Otevřeme si jej a na nové straně doplníme údaje.

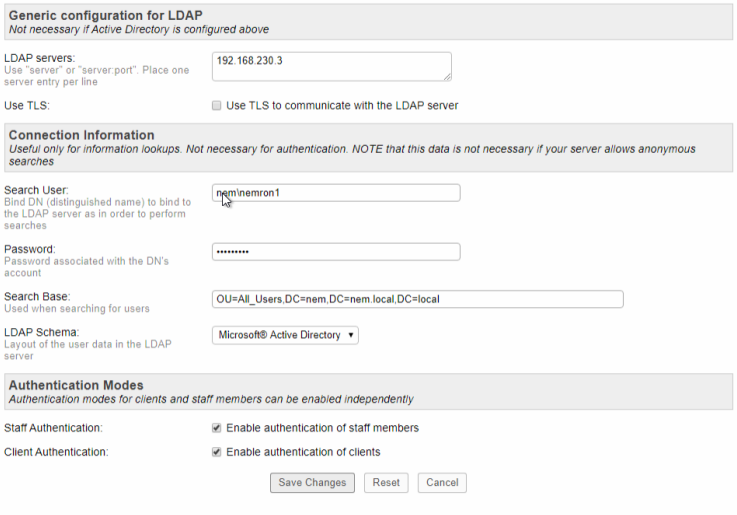


Obrázek 223 - Konfigurace osTicket č.2



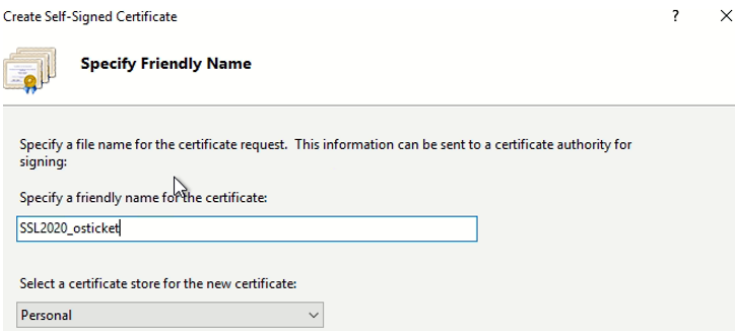
Obrázek 224 - Konfigurace osTicket č.3

Jako Default domain zvolíme nem.local, DNS server bude 192.168.230.3 a LDAP server 192.168.230.3. Dále ještě vložíme uživatele, pod kterým bude osTicket přistupovat k Active Directory serveru (nemron1). Zadáme heslo a poté Search Base (OU=All_Users, DC=nem, DC=nem.local, DC=local) a nastavení aplikujeme. [20]

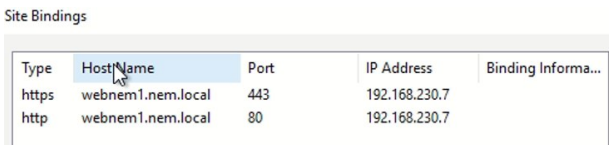


Obrázek 225 - Konfigurace osTicket č.4

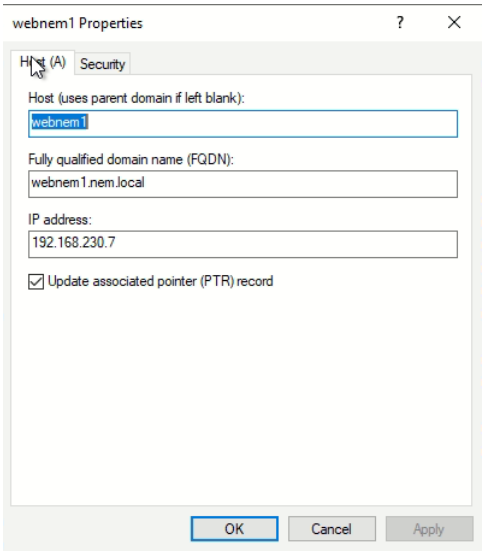
Stejně jako v případě webového serveru vytvoříme i pro web osTicket systému selfhosted SSL certifikát a přidáme DNS záznam, abychom nemuseli používat IP adresu pro připojení na tuto webovou aplikaci.



Obrázek 226 - Certifikát SSL



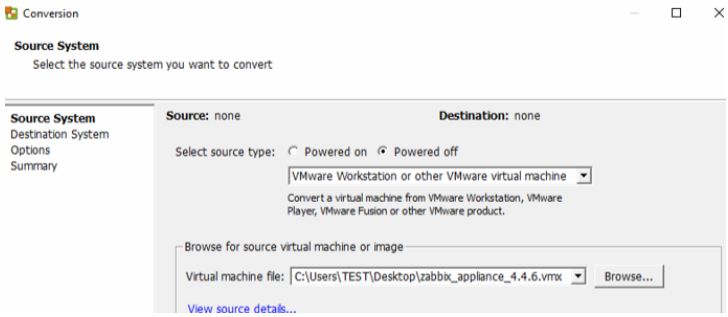
Obrázek 227 - Nastavení spojení



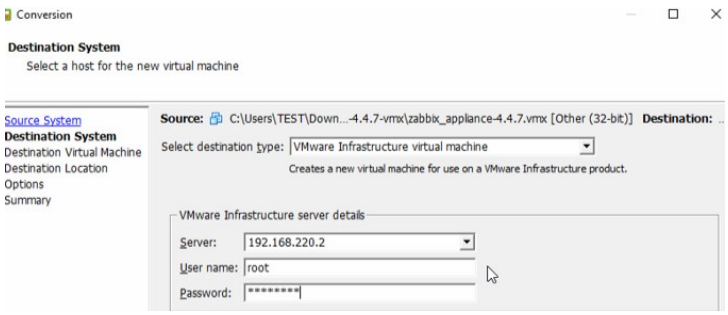
Obrázek 228 - Nastavení spojení č.2

18 INSTALACE MONITOROVACÍHO SERVERU

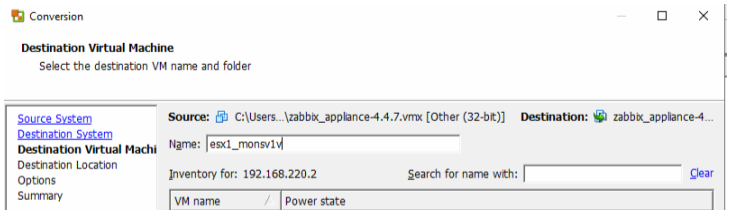
Pro instalaci monitorovacího serveru musíme nejprve stáhnout a upravit image vytvořenou zabbix týmem. Stáhneme zabbix appliance, která je dostupná na adrese „https://www.zabbix.com/download_appliance“, po dokončení stahování ještě musíme stáhnout VMware vCenter Converter Standoalone Client z webu „https://my.vmware.com/en/web/vmware/info/slug/infrastructure_operations_management /vmware_vcenter_converter_standalone/6_2_0“. Po nainstalování klienta jej otevřeme a vybereme File/Convert Virtual Machine. Na následujícím listu zvolíme typ systému virtuálního disku a náš stažený soubor s koncovkou „vmx“. Vyplníme údaje o našem ESXi hostu (192.168.220.2) a také root uživatele a heslo. Přiřadíme prostor na disku jako ostatním virtuálním strojům. Poté dokončíme konverzi a prvotní instalace serveru je hotová.



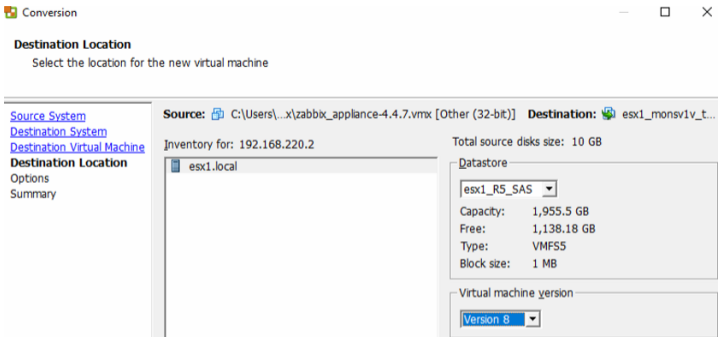
Obrázek 229 - Konverze obrazu disku pro VMware



Obrázek 230 - Konverze obrazu disku pro VMware č.2



Obrázek 231 - Konverze obrazu disku pro VMware č.3



Obrázek 232 - Konverze obrazu disku pro VMware č.4

18.1 Konfigurace Zabbix monitorovacího systému

Po dokončení zavedení systému se přihlásíme pomocí defaultního admin účtu appliance.

```
abbix login: appliance
assword:
ast login: Thu Mar  5 12:57:58 CET 2020 on tty1
ppliance@zabbix:~$ _
```

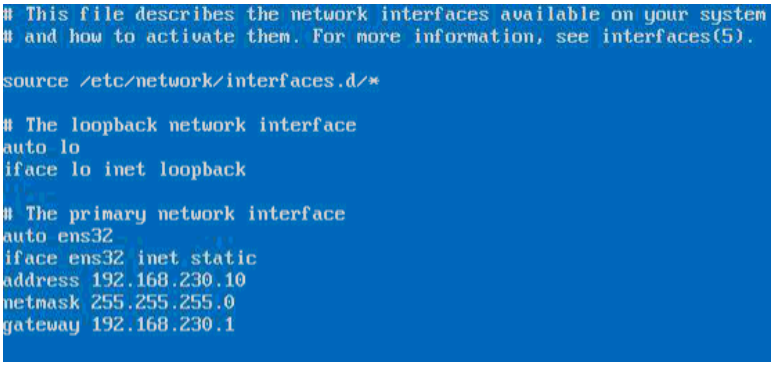
Obrázek 233 - Přihlášení Zabbix

Nejdříve změníme heslo účtu pomocí příkazu passwd.

```
root@zabbix:/home/appliance# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

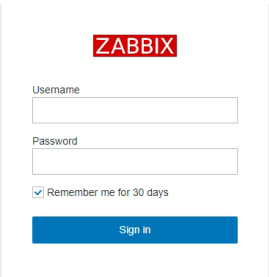
Obrázek 234 - Změna hesla

Dále je potřeba změnit naši IP adresu z dynamické (DHCP) na statickou adresu. To uděláme změnou v souboru ifcfg-eth0, který nalezneme v /etc/sysconfig/network-scripts/ifcfg-eth0. Použijeme k tomu textový editor mcedit. Nejprve však použijeme příkaz „sudo su“ abychom si přiřadili root oprávnění pro našeho uživatele. A upravíme následovně. Změníme „iface ens32 inet dhcp“ na „iface ens32 inet static“. Přidáme „address 192.168.230.10“, dále „netmask 255.255.255.0“ a „gateway 192.168.230.1“. [21]



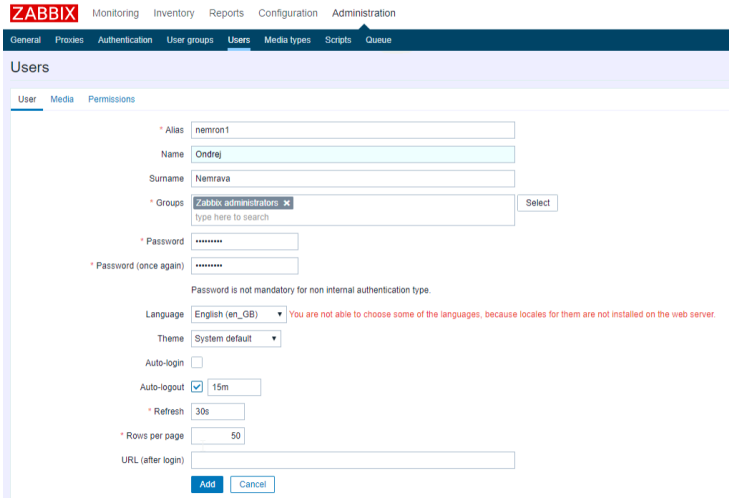
Obrázek 235 - Konfigurace síťového adaptéru

Pro konfiguraci DNS serveru musíme textovým editorem mcedit změnit ještě soubor /etc/resolv.conf, kde vložíme 192.168.230.3 jako náš DNS server. Po uložení změn použijeme příkazy ifdown ens32 && sudo ifup ens32. Následně provedeme update a upgrade serveru pomocí příkazů „apt-get update“ a „apt-get upgrade“. Poté nainstalujeme openVMtools, pomocí příkazu „apt-get install open-vpn-tools“. [21] Nyní si můžeme otevřít prohlížeč a zadat 192.168.230.10/zabbix, což je pro nás vstupní bod pro přístup do samotného frontendu Zabbix monitorovacího systému. Přihlásíme se pomocí defaultního uživatelského jména a hesla (Admin:zabbix).



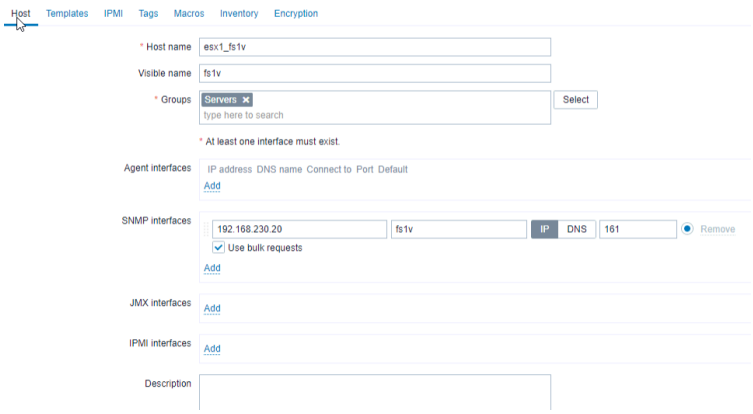
Obrázek 236 - Přihlášení do Zabbix konzole

Po přihlášení si vytvoříme nového uživatele (nemron1) zvolením nabídky Administration/Users, kde vybereme Vytvořit uživatele. Na nové stránce doplníme informace o uživateli a přidáme ho do skupiny Zabbix administrators. Poté jej vytvoříme. [21]

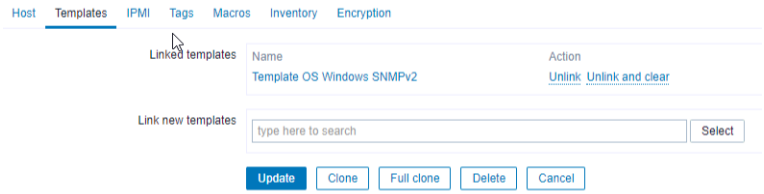


Obrázek 237 - Vytvoření administrátorského účtu

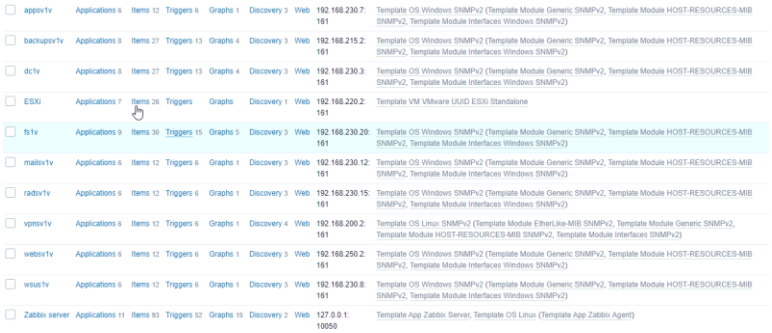
Nyní musíme nastavit přístupy a přiřadit monitorovací šablony pro všechny naše servery. Abychom mohli přidat naše servery, podíváme se do oddílu Configuration, kde zvolíme Hosts a dáme Create host. Vytvoříme nového hosta pro FS server. Doplníme název (esx1_fs1v), IP (192.168.230.20), DNS jméno esx1dc1v a taktéž přidáme SNMP rozhraní na stejnou IP a DNS jako má náš FS server. Stejně jako u tohoto serveru budeme postupovat u všech ostatních serverů, které budeme chtít monitorovat (v našem případě všechny). Na všechny vytvořené hosty musíme přiřadit správnou šablonu, pro Windows, to bude „Template OS Windows SNMPv2“ a pro systémy Linux „Template OS Linux SNMPv2“. [21]



Obrázek 238 - Konfigurace Zabbix monitoringu

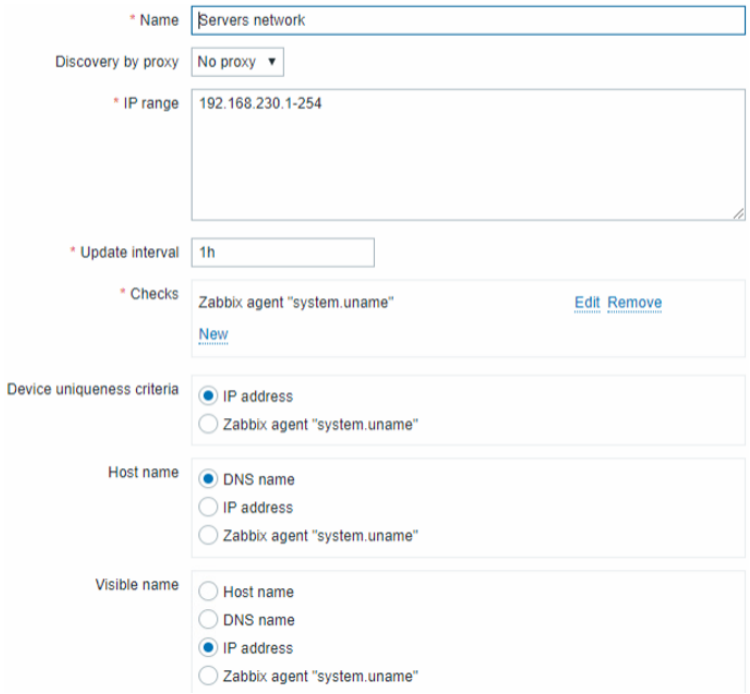


Obrázek 239 - Konfigurace Zabbix monitoringu č.2



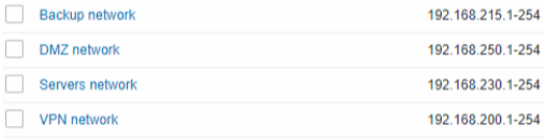
Obrázek 240 - Konfigurace Zabbix monitoringu č.3

Dále musíme nastavit pravidla, dle kterých může monitorovací server operovat a sbírat data. Rozklikneme si Configuration/Discovery, kde nastavíme Servers Network, zadáme IP rozsah 192.168.230.1-254, unikátní klíč bude IP adresa, hostname bude dle DNS a zobrazované jméno bude taktéž IP adresa.



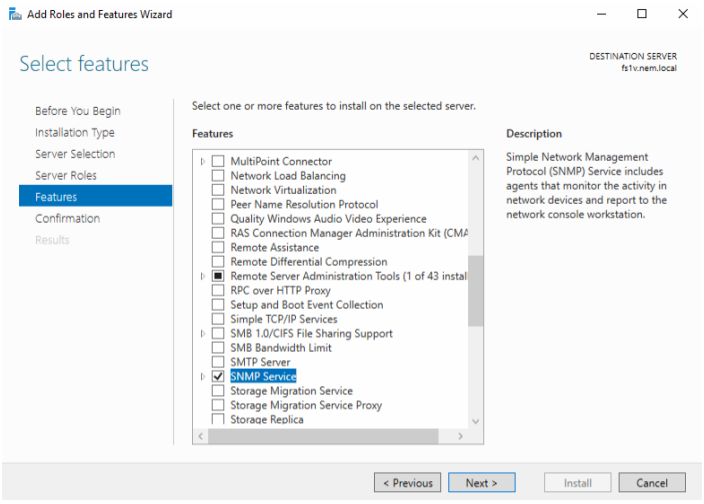
Obrázek 241 - Konfigurace Zabbix monitoringu č.4

Postupně přidáme všechny subnety, kde se nachází servery, které chceme monitorovat.



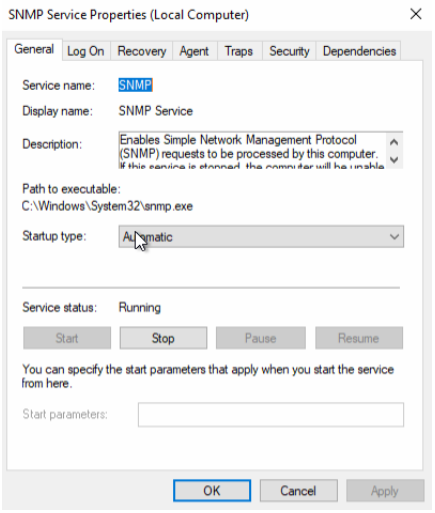
Obrázek 242 - Konfigurace Zabbix monitoringu č.5

Pro umožnění sběru dat přes SNMP budeme muset na všech našich serverech nainstalovat pomocí Server Manageru funkcionalitu SNMP a posléze konfigurovat.

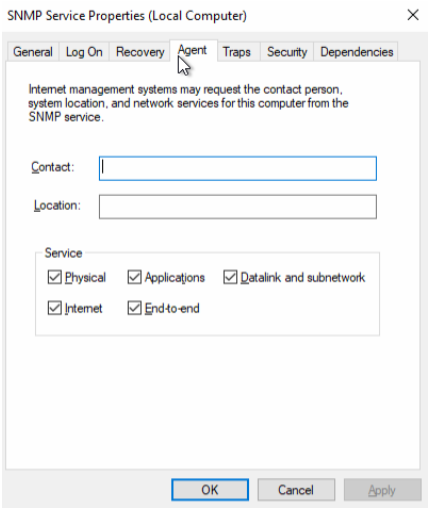


Obrázek 243 - Instalace SNMP

Po dokončení instalace otevřeme services.msc (popřípadě Services přes nabídku Start). Najdeme službu SNMP Service, kterou otevřeme, ověříme, že je zvolen automatický start. A následně zvolíme lištu „Agent“, kde pro potřeby monitorování zaškrtneme všechny pole.

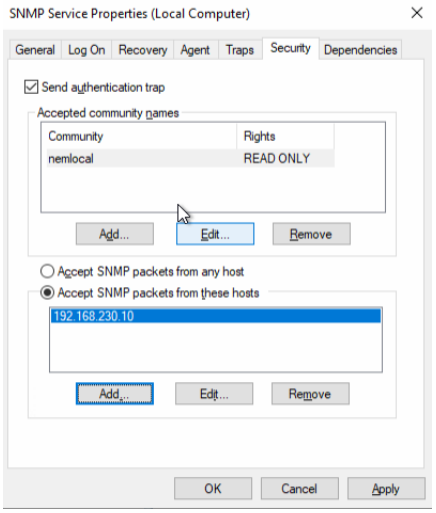


Obrázek 244 – SNMP konfigurace

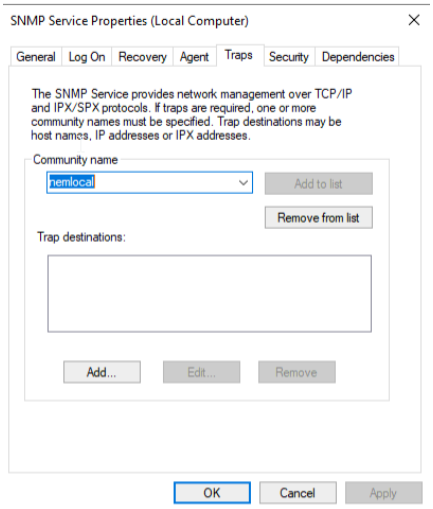


Obrázek 245 - SNMP konfigurace č.2

Následně otevřeme Security a zde vložíme naši doménu nemlocal a zvolíme pouze oprávnění pro čtení a přidáme IP adresu našeho monitoring serveru (192.168.230.10) mezi adresy odkud server bude přijímat SNMP pakety a zároveň přidáme náš community name do Traps pomocí Add to list. Takto to provedeme na všech Windows serverech.



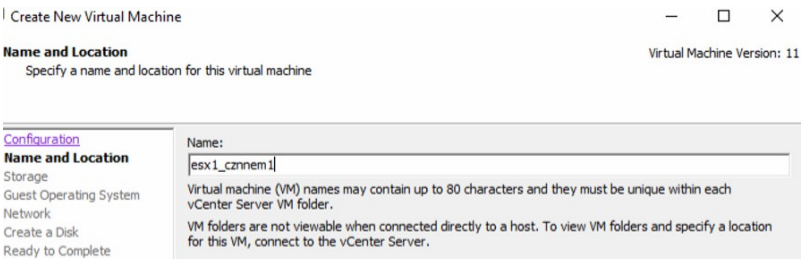
Obrázek 246 - SNMP konfigurace č.3



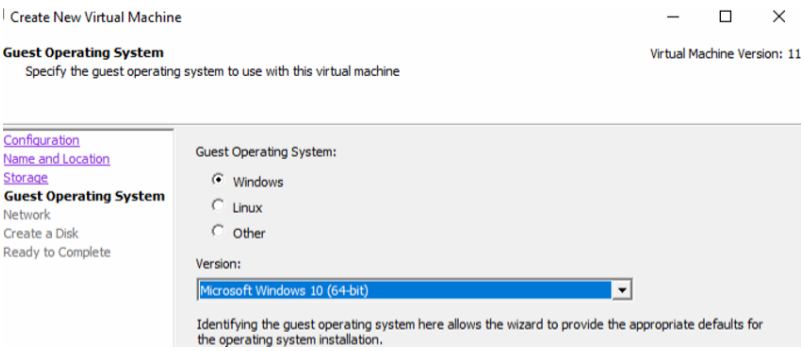
Obrázek 247 - SNMP konfigurace č.4

19 INSTALACE KLIENTŮ

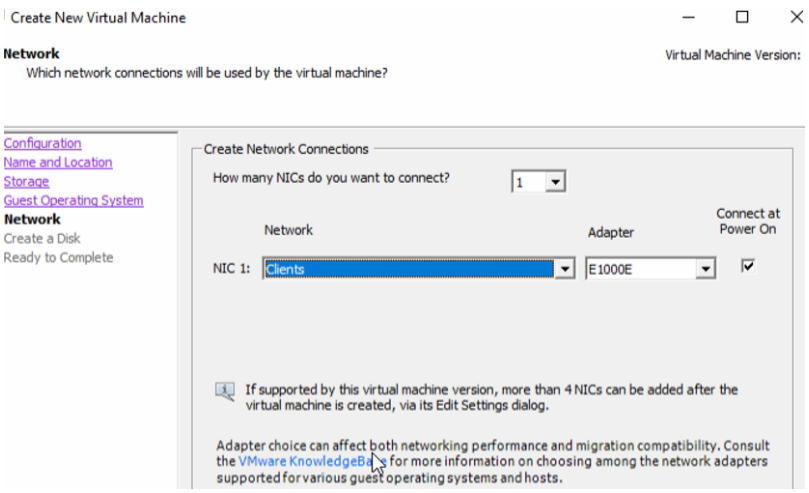
Instalaci klientů provedeme standardně, jako u serveru jen zvolíme jiný typ systému při tvorbě VM. Zároveň strojům nebudeme nastavovat statickou IP adresu, neboť budou mít přiřazenou IP adresu DHCP serverem. Samozřejmě budeme instalovat systém Windows 10 a nikoliv Windows Server 2019.



Obrázek 248 - Vytvoření klient VM

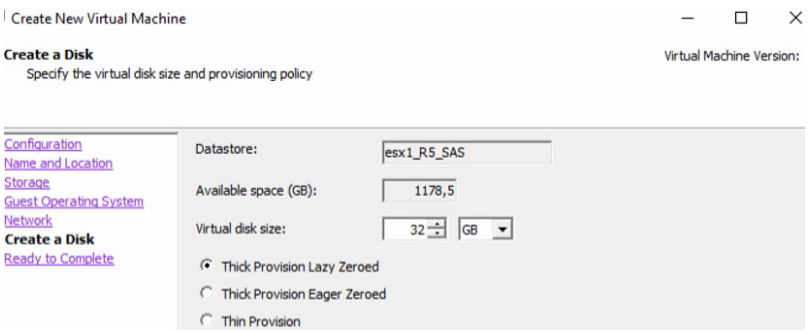


Obrázek 249 - Vytvoření klient VM č.2

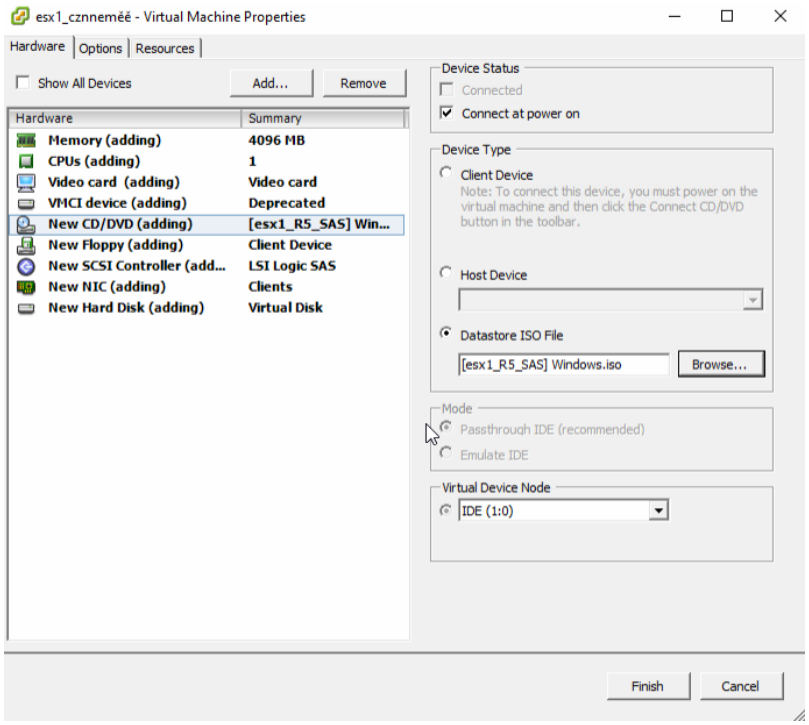


Obrázek 250 - Vytvoření klient VM č.3

Nebudeme virtuální stroje přiřazovat do port skupiny Servers, nýbrž Clients. Počítače následně přiřadíme do domény a zvolíme jména strojů (cznnem1 a cznnem2). Pro naše potřeby takto nainstalujeme 2 virtuální stroje, nicméně testy budeme následně pouštět z počítače mimo doménu, kde bude nahraný systém Linux a potřebné softwarové doplňky.



Obrázek 251 - Vytvoření klient VM č.4

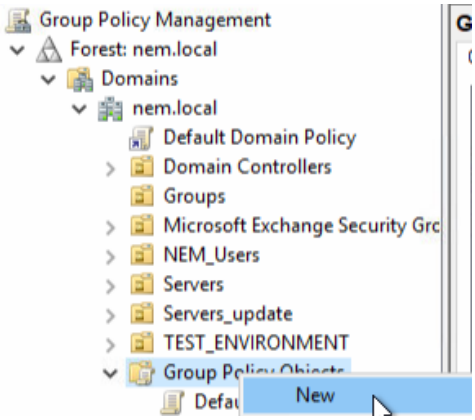


Obrázek 252 - Vytvoření klient VM č.5

Na obou počítačích taktéž povolíme RDP. Následně provedeme restart. Po restartu pak oba počítače přesuneme v Active Directory, mezi stroje, které se budou aktualizovat pomocí WSUS serveru.

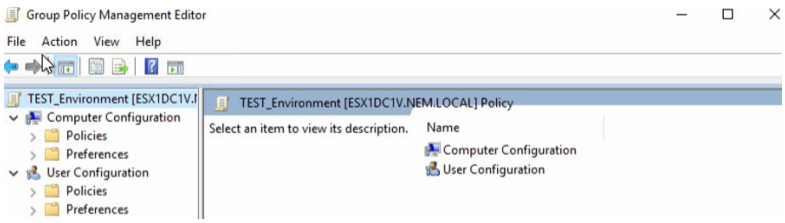
20 KONFIGURACE DOMÉNOVÝCH POLITIK

Pro nastavení veškerých politik, se připojíme pomocí RDP na náš DC server (192.168.230.3), kde otevřeme Group Policy Management, kde v oblasti Group Policy Objects vytvoříme nový objekt TEST_Environment.



Obrázek 253 - Vytvoření nové politiky

Následně pravým kliknutím zvolíme Edit a otevřeme tím nový interface Group Policy Management Editor. V základním okně vidíme 2 typy možných konfiguračních částí, kde v jedné budeme moci nastavit politiky pro stroje, a ve druhé naopak pro uživatele. Obě možností následně obsahují rozdělení na Policies a Preferences.



Obrázek 254 - Rozdělení politik

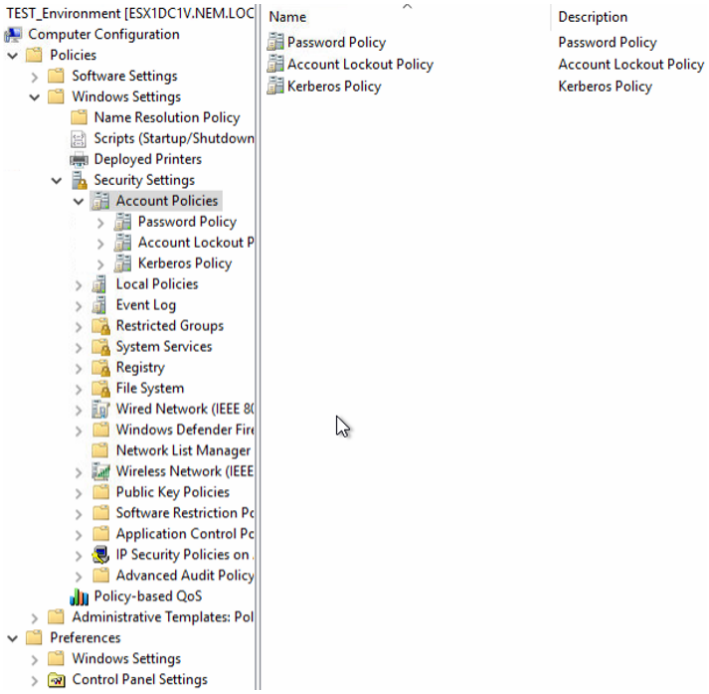
20.1 Computer Configuration policies

20.1.1 Security settings politiky

Prvně se podíváme do Computer Configuration a zde zvolíme policies, což nám rozšíří nabídku na Software, Windows a Administrative Templates (stejně tomu je i u User Configuration). Zde se podíváme do Windows settings a následně do Security settings. Otevřeme první oblast, což je Account policies. [23]

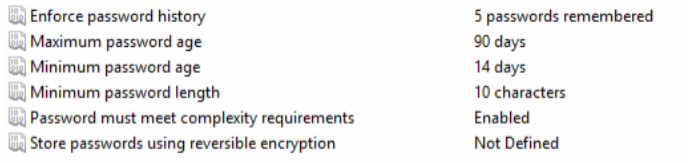
20.1.1.1 Account policies

Nyní nakonfigurujeme politiky pro hesla, lockout a Kerberos.

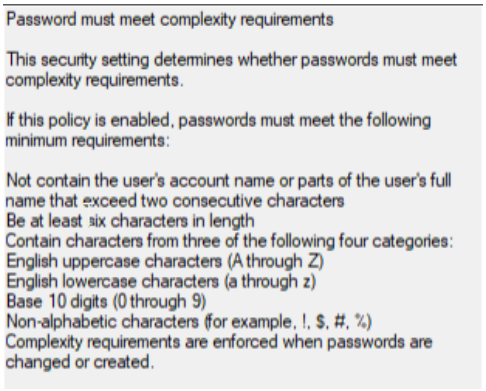


Obrázek 255 - Politiky účtů

Pro heslo nastavíme maximální stáří hesla 90 dní, minimální stáří 14 dní, nejkratší možnou délku 10 znaků a dále, že si bude AD pamatovat posledních 5 hesel, která se musí lišit. Taktéž povolíme komplexnost hesel, což jsou další požadavky na hesla jako nutnost obsahovat velké a malé znaky, číslo a další.



Obrázek 256 - Politiky účtů č.2

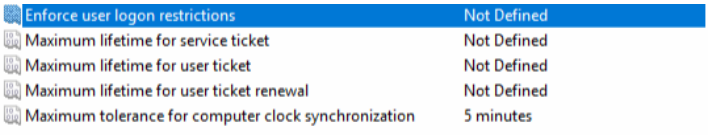


Obrázek 257 - Politiky účtů č.3

Pro Account lockdown, což je uzamčení Windows účtu při překročení počtu zadání špatného hesla například, zvolíme Lockout duration 0 (účet zůstane zamčený až do odemčení administrátorem systému). K uzamčení dojde po 5 špatných pokusech a reset počítadla špatně zadaného hesla po 10 minutách.

Obrázek 258 - Uzamčení účtu

V rámci Kerberos ponecháme téměř vše na defaultních hodnotách, změníme pouze maximální toleranci pro nesynchronizovaný čas mezi serverem a klientem na 5 minut.



Obrázek 259 - Kerberos politiky

20.1.1.2 Local policies

Dále se přesuneme do Local policies a v Audit policy změníme pouze hodnoty u auditů account logon events a logon events (oboje na Success a Failure), abychom mohli sledovat, kam se uživatel hlásil ať již úspěšně či nikoliv (posléze vhodné pro dohledávání, kde se uživatelský účet uzamyká).

Audit account logon events	Success, Failure
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

Obrázek 260 - Audit politiky

Nyní se přesuneme do User Rights Assignment, kde pouze u některých politik přidám AD skupinu Domain Admins, abychom rozšířili pravomoc této skupiny. Zbytek ponecháme v původním nastavení.

Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Administrators
Act as part of the operating system	Not Defined
Add workstations to domain	Domain Admins,Administrators
Adjust memory quotas for a process	Administrators
Allow log on locally	Domain Admins,Administrators
Allow log on through Remote Desktop Services	Domain Admins,Administrators
Back up files and directories	Not Defined
Bypass traverse checking	Not Defined
Create a pagefile	Not Defined
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Users
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delega...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Impersonate a client after authentication	SERVICE,Domain Admins,Admi...

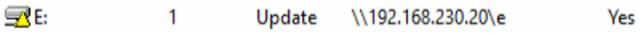
Obrázek 261 - Admin práva politiky

V rámci další kategorie (Security Options) změníme vícero politik, jako například nastavení stejných požadavků na hesla jako jsme již udělali u lokálních politik a další.

Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Users can't add Microsoft accounts
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Disabled
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when ...	Not Defined
Domain member: Disable machine account password chan...	Not Defined
Domain member: Maximum machine account password age	90 days
Domain member: Require strong (Windows 2000 or later) se...	Not Defined
Interactive logon: Display user information when the session...	User display name only
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Disabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	5 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in c...	0 logons
Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Enabled
Interactive logon: Require Windows Hello for Business or sm...	Not Defined

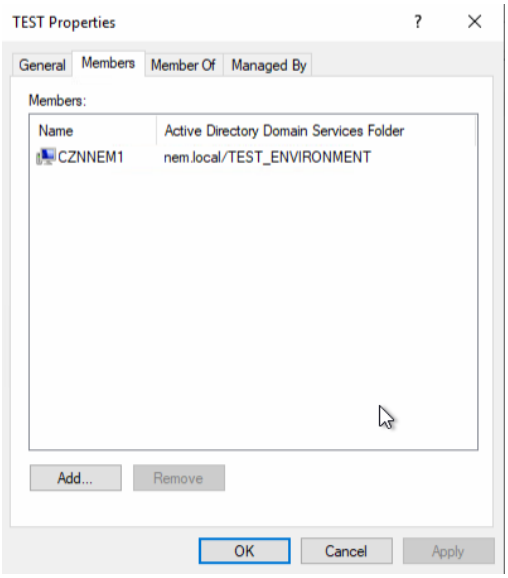
Obrázek 262 - Přihlašovací politiky

Přeskočíme kategorie Event log a přidáme do Restricted Groups, skupinu Blocked Users (což bude skupina pro propuštěné uživatele, či uživatele podezřelé z vynášení dat a podobných nežádoucích zakázaných činností). Dále již přejdeme do User Configuration, kde zvolíme Preferences, Windows Settings a Drive maps, kde vytvoříme novou cestu k našemu fileserveru, aby měli uživatelé přístup na sdílená data (192.168.230.20) pojmenujeme jej Disk E.



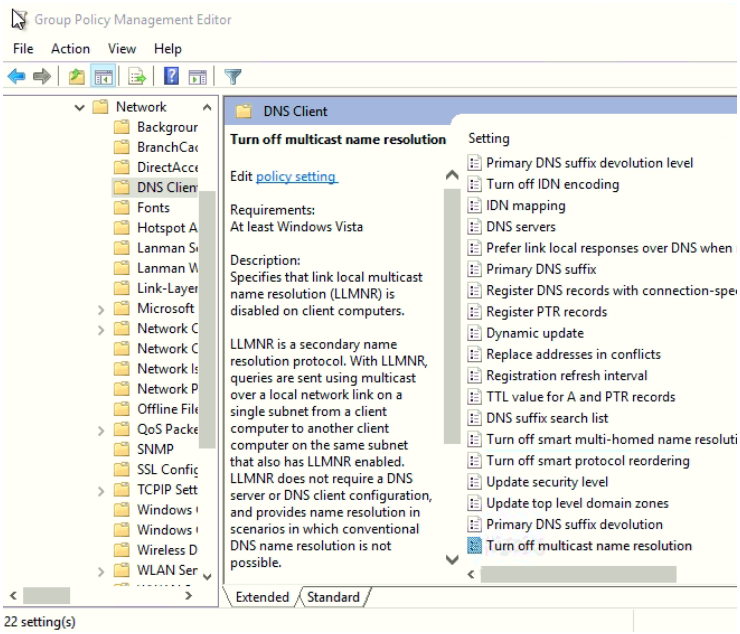
Obrázek 263 - Mapování síťového disku

Samozřejmě Windows politiky nám umožňují modifikovat a směrovat celou řadu dalších věcí, nicméně pro naše testovací prostředí, bude základní nastavení stačit. Teď již stačí jen politiky aplikovat pomocí přidání chtěných počítačů do této skupiny na Active Directory, popřípadě je přesunout do OU, abychom měli přehled, na které zařízení jsou aplikované politiky.



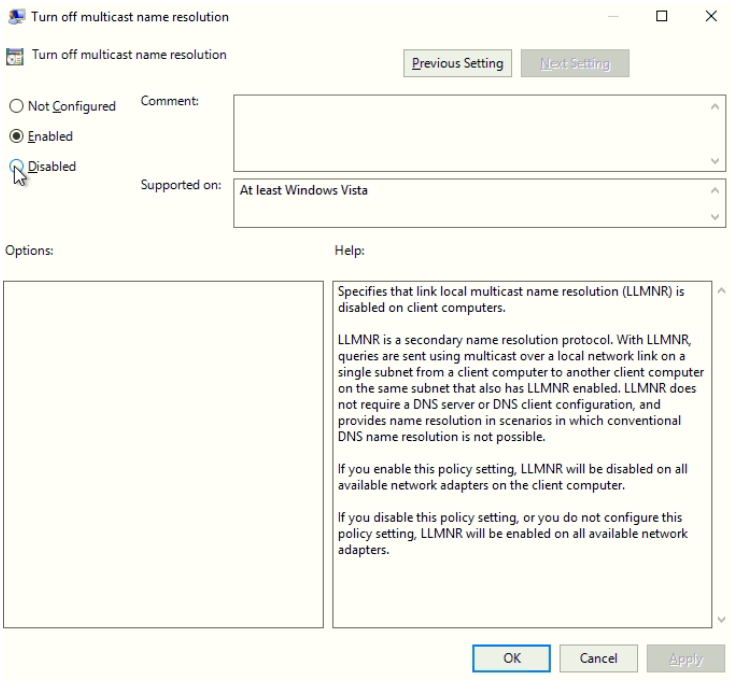
Obrázek 264 - Přidání zařízení do politiky

Další důležitou politikou, kterou je nutné použít je „Turn off multicast name resolution“, kde zvolíme Enabled, čímž zabráníme LLMNR poisoning útokům vůči SMB protokolu. Je ovšem nutné zároveň zakázat NetBIOS over TCP/IP, což uděláme na DHCP serveru, kde tuto možnost zakážeme.

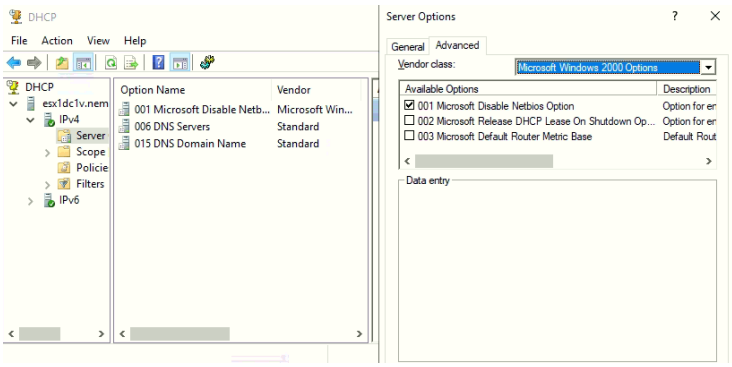


Obrázek 265 - Zakázání multicast name resolution

Otevřeme si Server Options a zde pravým tlačítkem myši otevřeme Configure options, následně menu Advanced, kde zvolíme Vendor class Microsoft Windows 2000 Options a zaškrtneme 001 Microsoft Disable NetBios Option a změníme defaultní hodnotu na 0x2.



Obrázek 266 - Zakázání NetBios



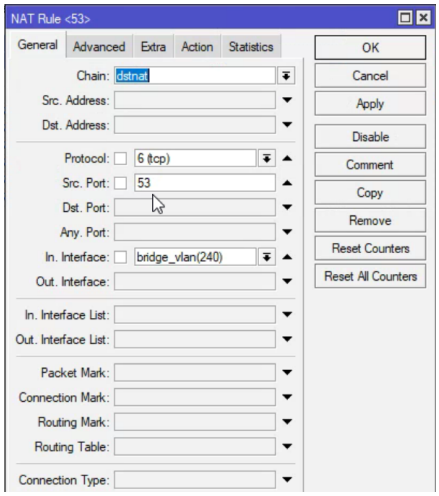
Obrázek 267 - Zakázání NetBios č.2

21 KONFIGURACE FIREWALLU

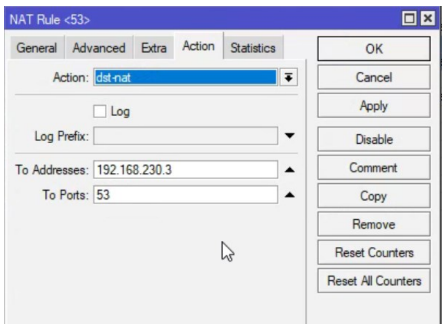
Firewall budeme dle zadání konfigurovat přímo na Mikrotikovém L3 switchi, který nám tuto potřebu více nežli dobře splní pro testovací účely. Samozřejmě v praxi bychom použili separátní server, který by zajišťoval ochranu našeho prostředí. Připojíme se proto pomocí winboxu na náš Mikrotik, kde jsme již v kapitole 4.1 provedli prvotní zabezpečení. Nyní se po přihlášení podíváme do kategorie IP a následně Firewall, kde jsme již vytvářeli pravidla NAT, nicméně nyní se budeme víceméně pohybovat v podmenu Filter Rules.

21.1 Force DNS, DHCP server

Prvním krokem bude vytvoření dst-nat pravidel pro DNS a DHCP služby, abychom zamezili nastrčeným „serverům“, které poskytují stejné služby. Zvolíme tedy menu „NAT“, kde vytvoříme pravidla pro klientské bridge a posléze provedeme stejné kroky pro bridge serverové. Nejprve vybereme chain dst-nat a cílový port 53 protokolu TCP (který je využíván DNS službou), doplníme rozhraní bridge_vlan(240) a přesuneme se do podmenu Action, kde vybereme akci dst-nat a do polí vložíme IP adresu našeho DNS serveru a cílový port.

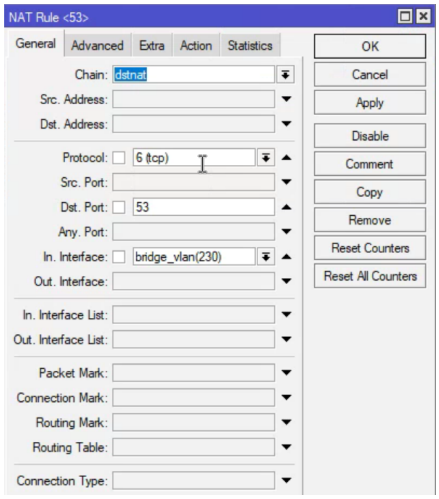


Obrázek 268 - NAT pravidlo (53)

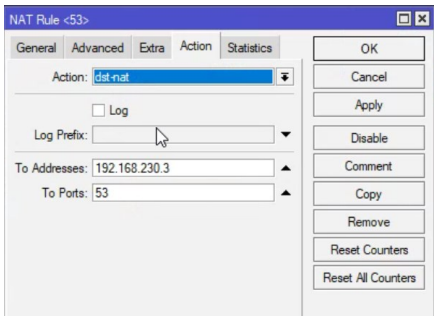


Obrázek 269 - NAT pravidlo (53) č.2

Následně vytvoříme stejné pravidlo pro druhý bridge.

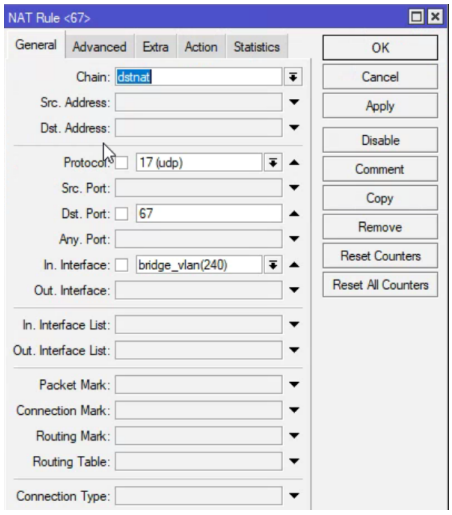


Obrázek 270 - NAT pravidlo (53) č.3

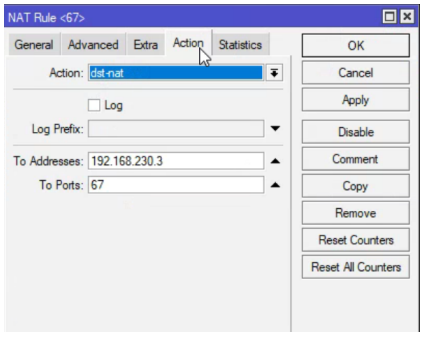


Obrázek 271 - NAT pravidlo (53) č.4

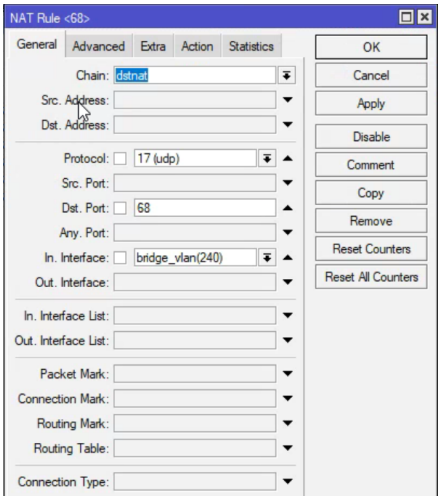
Stejným způsobem definujeme pravidla pro DHCP server, kde ovšem zahrneme pouze klientský bridge, neboť servery mají přiřazenou statickou IP adresu. Zde zvolíme opět dst-nat dst. portu 67 protokolu UDP na rozhraní bridge_vlan(240) a akci dst-nat s cílem IP serveru 192.168.230.3 a cílového portu 67. Totéž následně provedeme pro druhý port využívaný DHCP službou a to port 68. Samozřejmě všechny pravidla řádně okomentujeme, neboť v případě následných úprav by práce s neokomentovanými pravidly byla více než nepřehledná.



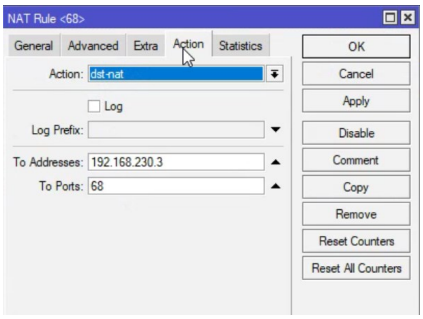
Obrázek 272 - NAT pravidlo (67)



Obrázek 273 - NAT pravidlo (67) č.2



Obrázek 274 - NAT pravidlo (68)



Obrázek 275 - NAT pravidlo (68) č.2

21.2 Filter Rules

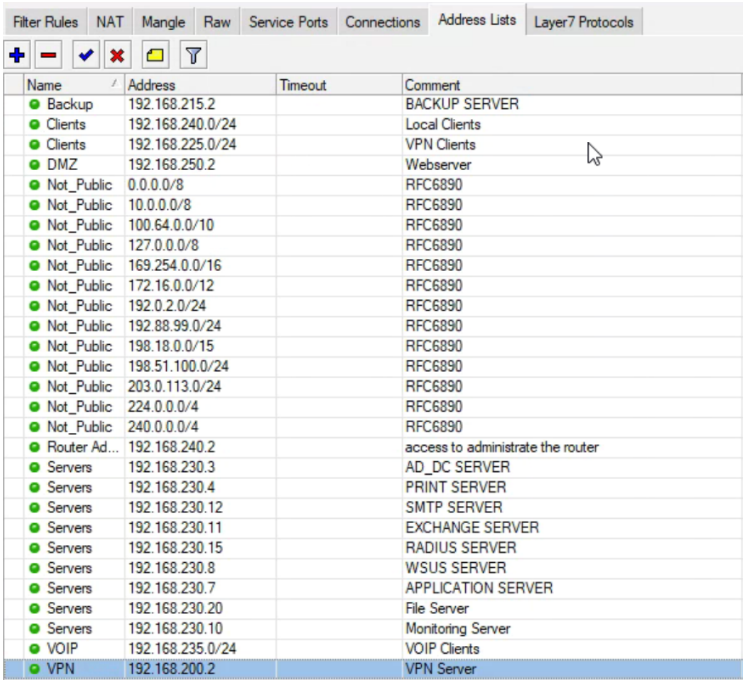
Nyní se posuneme do podmenu Filter Rules, kde budeme konfigurovat filtrační pravidla firewallu. Existují dvě možnosti přístupu k tvorbě firewallu. První strategie povolí všechen síťový provoz, kromě toho, jež je zakázán a druhá strategie funguje přesně naopak, kdy zakážeme veškerý provoz, kromě explicitně povoleného. Budeme využívat druhé možnosti, neboť poskytuje větší bezpečnost a zamezuje alespoň částečně vliv lidského faktoru. Prvně si vytvoříme adresní listy pro jednodušší práci s pravidly. Pro každý záznam zvolíme název, který následně spojuje dané prvky do skupin. Je potřeba zvolit adresní rozsah, či konkrétní IP adresu zadávané součásti síťové infrastruktury. Vytvoříme tak adresní listy pro:

- Backup – Backup Server
- Klienty – Lokální klienti, VPN klienti
- DMZ - Webserver
- Servery – DC, Fileserver, Aplikační server a další.
- VOIP – VOIP klienti
- VPN – VPN server

Následně si vytvoříme seznam pro Not_Public, kde zavedeme IP adresy, které by se neměly nacházet ve vnější síti, pro zvýšení bezpečnosti našeho systému. Zde zavedeme adresní rozsahy: [16]

- 0.0.0.0/8
- 10.0.0.0/8

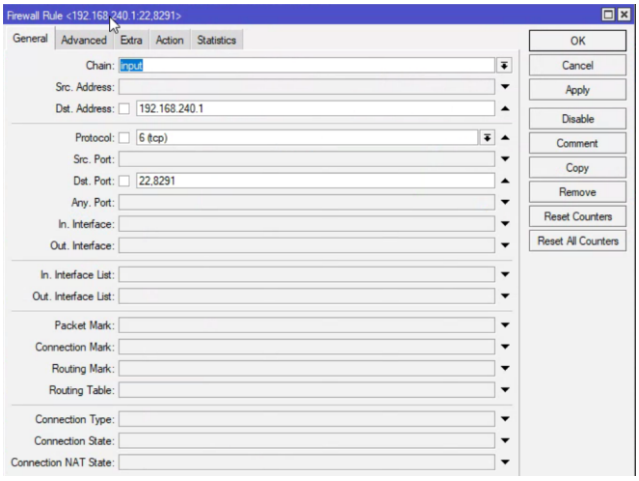
- 100.64.0.0/10
- 127.0.0.0/8
- 169.254.0.0/16
- 172.16.0.0/12
- 192.0.2.0/24
- 192.88.99.0/24
- 198.18.0.0/15
- 198.51.100.0/24
- 203.0.113.0/24
- 224.0.0.0/4
- 240.0.0.0/4



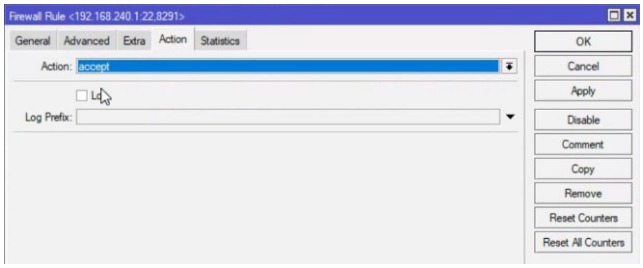
Name	Address	Timeout	Comment
Backup	192.168.215.2		BACKUP SERVER
Clients	192.168.240.0/24		Local Clients
Clients	192.168.225.0/24		VPN Clients
DMZ	192.168.250.2		Webserver
Not_Public	0.0.0.0/8		RFC6890
Not_Public	10.0.0.0/8		RFC6890
Not_Public	100.64.0.0/10		RFC6890
Not_Public	127.0.0.0/8		RFC6890
Not_Public	169.254.0.0/16		RFC6890
Not_Public	172.16.0.0/12		RFC6890
Not_Public	192.0.2.0/24		RFC6890
Not_Public	192.88.99.0/24		RFC6890
Not_Public	198.18.0.0/15		RFC6890
Not_Public	198.51.100.0/24		RFC6890
Not_Public	203.0.113.0/24		RFC6890
Not_Public	224.0.0.0/4		RFC6890
Not_Public	240.0.0.0/4		RFC6890
Router Ad...	192.168.240.2		access to administrate the router
Servers	192.168.230.3		AD_DC SERVER
Servers	192.168.230.4		PRINT SERVER
Servers	192.168.230.12		SMTP SERVER
Servers	192.168.230.11		EXCHANGE SERVER
Servers	192.168.230.15		RADIUS SERVER
Servers	192.168.230.8		WSUS SERVER
Servers	192.168.230.7		APPLICATION SERVER
Servers	192.168.230.20		File Server
Servers	192.168.230.10		Monitoring Server
VOIP	192.168.235.0/24		VOIP Clients
VPN	192.168.200.2		VPN Server

Obrázek 276 - Address Lists

Dále si vytvoříme pravidlo pro přístup z našeho Admin stroje, abychom si špatně zvoleným pravidlem nezakázali přístup k routeru. Zvolíme si řetězec input, protože se budeme připojovat přímo k routeru, zadáme adresu routeru do Dst. Address (192.168.240.1), vybereme protokol TCP a port 22, 8291, což jsou porty pro SSH a WinBox připojení k routeru. V menu Action zvolíme Accept.

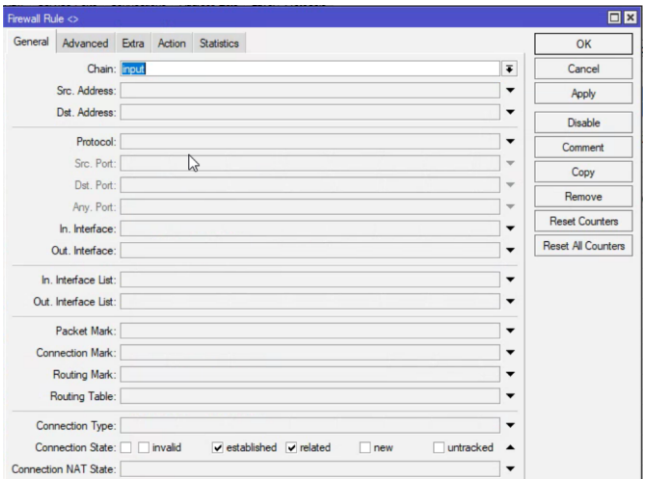


Obrázek 277 - Firewall input (22,8291)

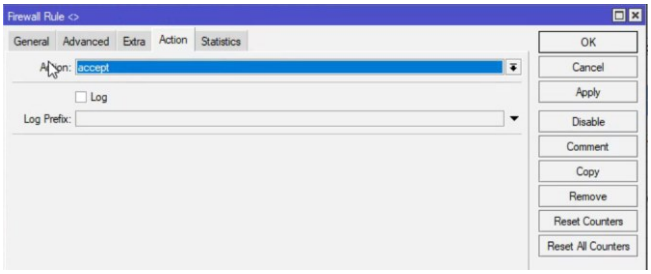


Obrázek 278 - Firewall input (22,8291) č.2

Dalšími budou pravidla ulehčující práci routeru, neboť pokaždé když by procházela komunikace routerem, musel by projít veškerá pravidla a teprve poté propustit komunikaci dál, nicméně to je velmi náročné na výpočetní výkon routeru, a tudíž za pomocí těchto pravidel již router nebude muset kontrolovat veškerou komunikaci u připojení, která již jsou navázána a otestována vůči firewallu.

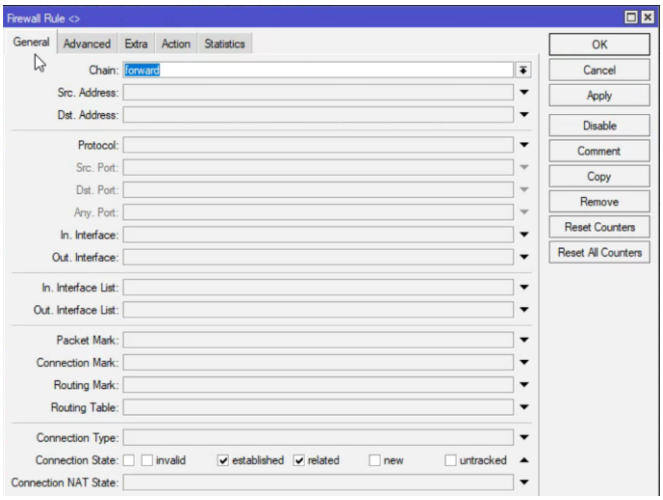


Obrázek 279 - Firewall established, related input

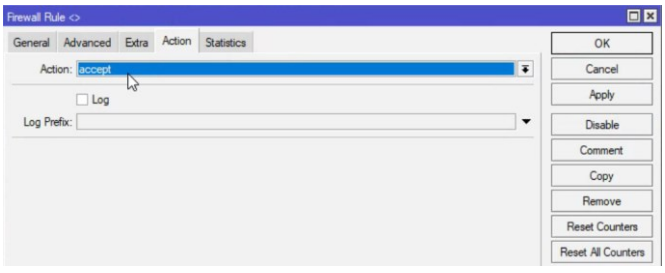


Obrázek 280 - Firewall established, related input č.2

Zvolíme si řetězec input pro veškerou vstupní komunikaci mířící přímo na router a zaškrtneme established a related, v kategorii Action pak vybereme Accept. Což nám zaručí přijetí packetu, který pochází z připojení, které již bylo navázáno a zkontrolováno. Tudíž router nemusí stále dokola projíždět všechna pravidla firewallu. Stejně tak vytvoříme totéž pravidlo pro řetězec forward, který bude mít na starost veškerou komunikaci mířící na některé rozhraní v naší interní síti. Obě pravidla okomentujeme.

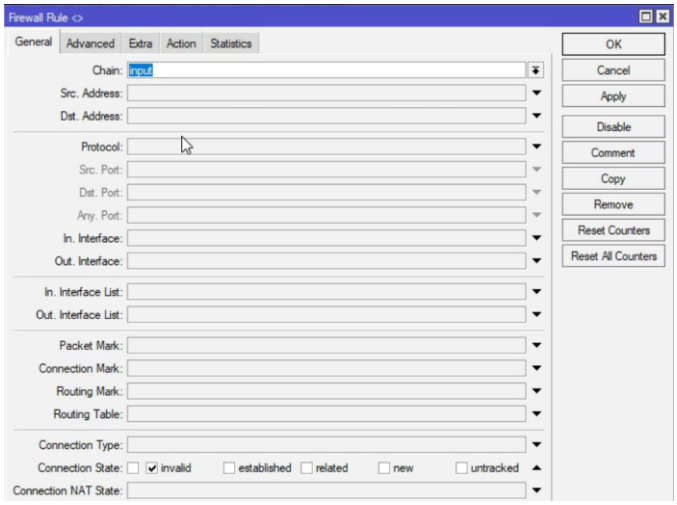


Obrázek 281 - Firewall established, related forward

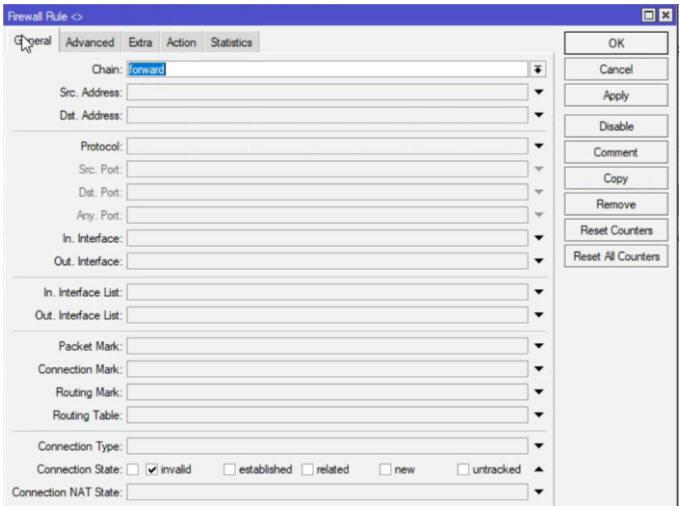


Obrázek 282 - Firewall established, related forward č.2

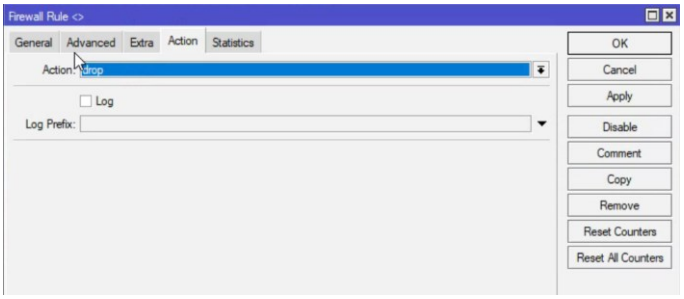
Dalšími pravidly budou Drop invalid packets, které budou nepřijímat veškeré neplatné pakety jak pro chain input, tak forward.



Obrázek 283 Firewall input invalid



Obrázek 284 - Firewall forward invalid



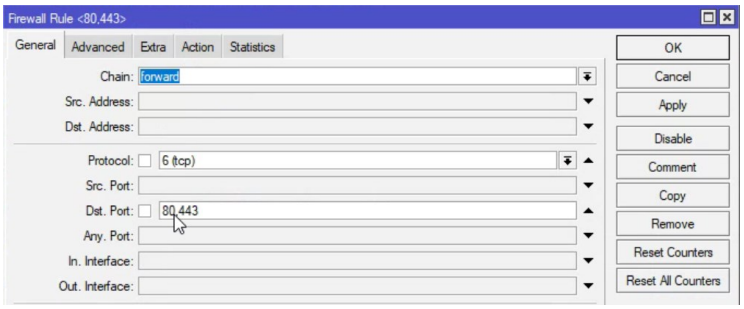
Obrázek 285 - Firewall forward/input invalid drop

Následně vyřadíme packety:

- které nejsou směrované na konkrétní IP adresu (input)
- které nemají zdrojovou IP adresu typu unicast (input)
- které jsou z vnější sítě, nicméně by tam neměly existovat (input)
- které jsou z vnější sítě, ale nejsou dst-natted (forward)
- které jsou z vnitřní sítě mířící do internetu, nicméně na adresu, které by neměla ve vnější síti existovat
- které jsou z vnější sítě, nicméně by tam neměly existovat (forward > všechny interfaces)
- které, jsou z vnitřní sítě, ale nemají interní IP adresu [16]

Obrázek 286 - Drop bogon pravidla

Dále povolíme průchod komunikaci na TCP portech 80,443 pro klienty a DMZ.



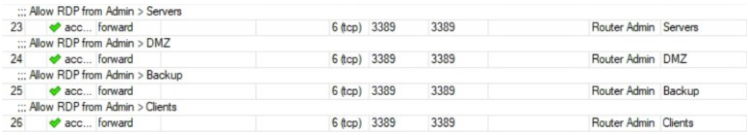
Obrázek 287 - DMZ (80,443) accept

Obrázek 288 - DMZ (80,443) accept č.2

Obrázek 289 - DMZ (80,443) accept č.3

Obrázek 290 - DMZ (80,443) accept č.4

Povolíme RDP připojení k našim zařízením, neboť nemáme k dispozici jiný software pro konektivitu. Tudíž pro stroje z Admin listu otevřeme TCP porty 3389 v rámci adresních listů Servers, DMZ, Backup, Clients.

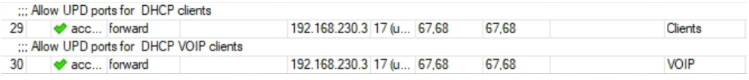


Obrázek 291- RPD accept z Router Admin zařízení

Pro servery na bázi Linuxové distribuce povolíme připojení pomocí SSH, což je TCP port 22.

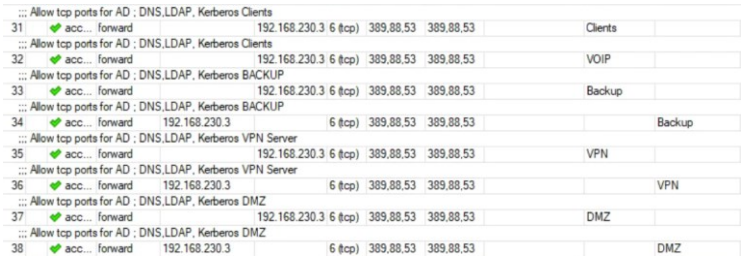
Obrázek 292 - SSH accept z Router Admin zařízení

Následně povolíme komunikaci na UDP portech 67,68 pro DHCP klienty a VOIP klienty.



Obrázek 293 - DHCP port accept

Dále otevřeme porty pro AD, DNS na našem DC serveru v rámci subnetů Clients, VOIP, Backup, VPN a DMZ. Kde pro Backup, VPN a DMZ musíme pravidla vytvořit oboustranně. Jedná se o TCP porty 389,88,53.



Obrázek 294 - AD, DNS ports povolení

Dalším krokem bude otevření SMB portů pro sdílení souborů mezi klienty a File-serverem. Potřebujeme TCP porty 139,445 a udp 137,138.

Obrázek 295 - SMB ports

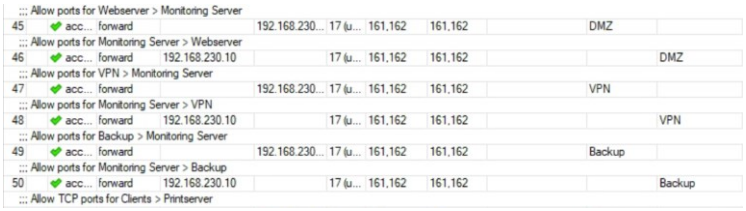
Otevřeme přístup pro klienty na portech 443,80 na aplikační server, aby byl dostupný ticketovací systém.

Obrázek 296 - Aplikační server 80,443 klient povoleno

Pokračujeme s otevřením portů pro emailové služby a to port 25 pro příchozí emaily z vnější sítě a následně porty pro IMAP, POP3, SMTP a přístupy klientů na emailové servery.

Obrázek 297 - Email port otevřen

Následně otevřeme komunikaci pro monitorovací server na DMZ, VPN a Backup subnetech, kdy je ve všech případech nutné otevřít porty na obou stranách a to konkrétně 161 a 162 což jsou porty pro SNMP a SNMPTRAP.



Obrázek 298 - Zabbix monitoring porty

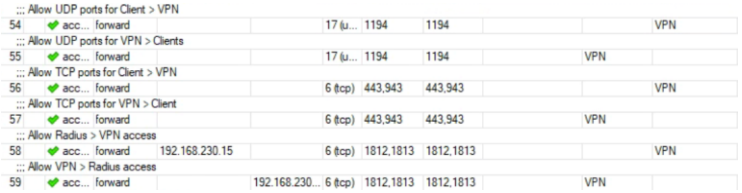
Dále otevřeme porty pro tiskové služby v rámci klientských subnetů.

Obrázek 299 - Porty pro tiskové služby na klientech

Dalším bodem je povolení komunikace VPN serveru se službou DHCP, a tudíž otevřeme UDP porty 67,68 pro umožnění přidělování adres VPN klientům.

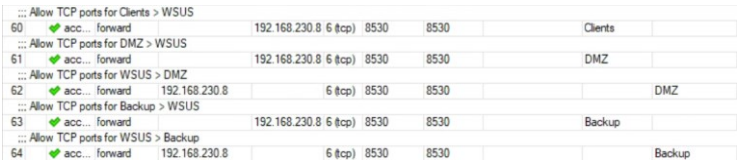
Obrázek 300 - VPN DHCP porty

Dalším krokem pro umožnění funkčnosti VPN serveru je povolení komunikace vnějších klientů s VPN serverem (UDP 1194, TCP 443, 943) a následně komunikaci VPN serveru s Radius serverem (TCP 1812, 1813).



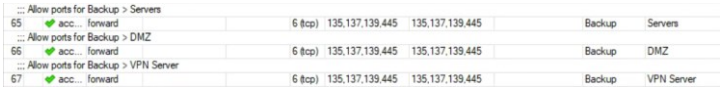
Obrázek 301 - VPN připojení porty

V rámci následujících pravidel povolíme přístup WSUS serveru ke klientům, DMZ, Backup a VPN Vlanům a naopak. Veškerý provoz je na TCP portech 8530.



Obrázek 302 - WSUS porty

Posledními Accept pravidly budou filtry pro zálohovací server a jeho přístup k jednotlivým subnetům z důvodu záloh a obnovení. Je nutné otevřít TCP porty 135, 137, 139, 445.



Obrázek 303 - Backup porty

Nyní se podíváme na finální „zahazovací“ pravidla, která nám zajistí, že nebudeme přijímat jiné síťové pakety a povolovat jiný síťový provoz nežli námi povolený. Zamezíme provozu mezi veškerými subnety, kromě výše povolených pravidel a mezi subnety Servers a Clients, ne však naopak. Veškerá pravidla řádně okomentujeme.

Obrázek 304 - Zahazovací pravidla

;;; Drop all trafic from VOIP > Clients								
91	drop	forward					VOIP	Clients
;;; Drop all trafic from VOIP > DMZ								
92	drop	forward					VOIP	DMZ
;;; Drop all trafic from VOIP > Servers								
93	drop	forward		192.168.230...			VOIP	
;;; Drop all trafic from VOIP > VPN								
94	drop	forward					VOIP	VPN
;;; Drop all trafic from VPN Clients > Servers								
95	drop	forward	192.168.225.0/24	192.168.230...				
;;; Drop all trafic from VPN Clients > VOIP								
96	drop	forward	192.168.225.0/24					VOIP
;;; Drop all trafic from VPN Clients > DMZ								
97	drop	forward	192.168.225.0/24					DMZ
;;; Drop all trafic from VPN Clients > Clients								
98	drop	forward	192.168.225.0/24	192.168.240...				
;;; Drop all trafic from VPN Clients > Backup								
99	drop	forward	192.168.225.0/24					Backup
;;; Drop all trafic from Clients > VPN Clients								
100	drop	forward	192.168.240.0/24	192.168.225...				
;;; Drop all trafic from Clients > Backup								
101	drop	forward	192.168.240.0/24					Backup
;;; Drop all trafic from Clients > DMZ								
102	drop	forward	192.168.240.0/24					DMZ
;;; Drop all trafic from Clients > VPN								
103	drop	forward	192.168.240.0/24					VPN
;;; Drop all trafic from Clients > VOIP								
104	drop	forward	192.168.240.0/24					VOIP
;;; Drop all trafic from Clients to Servers								
105	drop	forward	192.168.240.0/24					Servers

Obrázek 305 - Zahazovací pravidla č.2

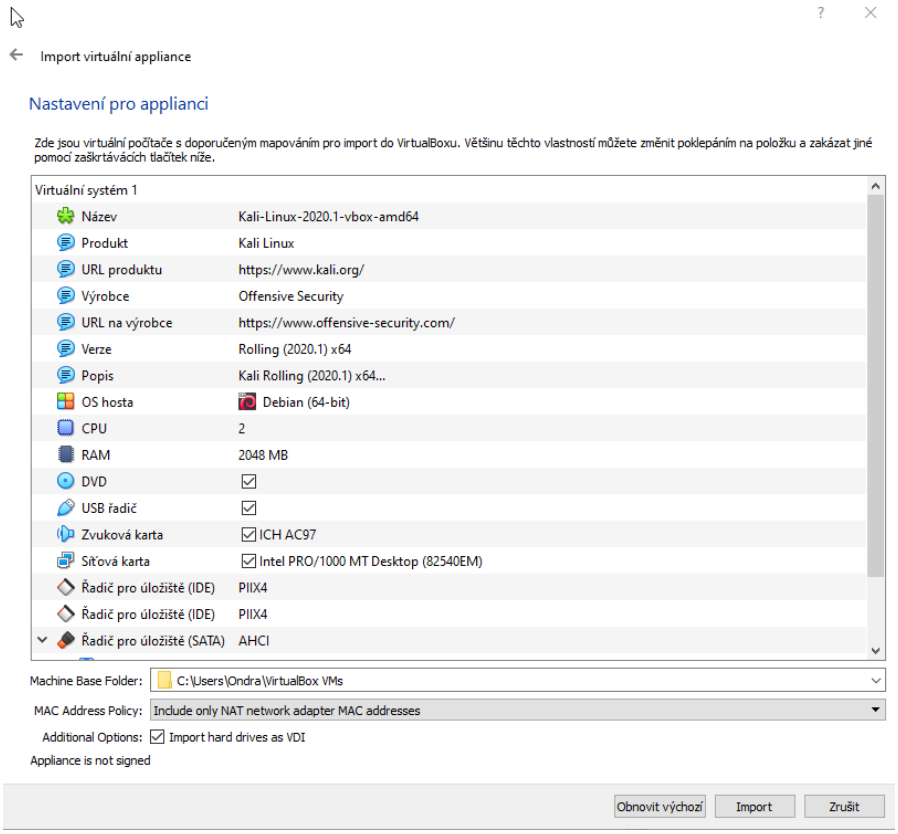
Dále přidáme ještě poslední pravidla pro vyřazení všech ostatních nechtěných portů.

!16	drop	input					
!17	drop	forward		6 (tcp)	!80,443,25	!80,443,25	Internet
!18	drop	forward		17 (udp)	!1194	!1194	Internet

Obrázek 306 - Zahazovací pravidla č.3

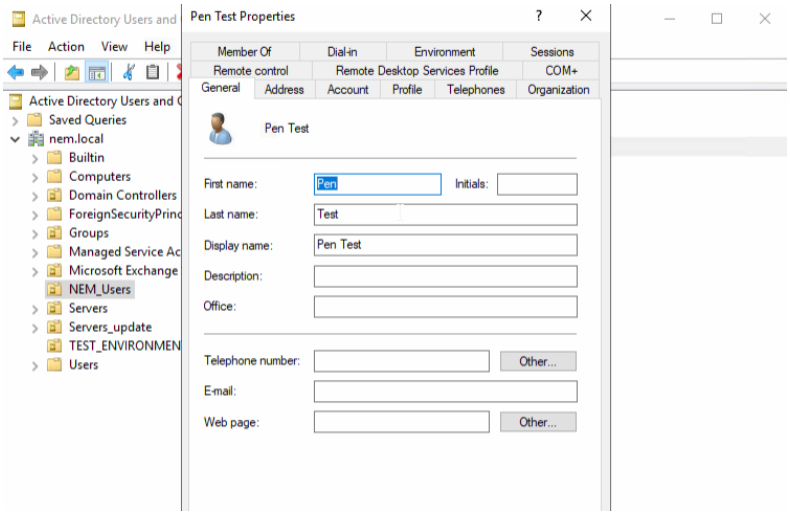
22 PENETRAČNÍ TESTY

Pro potřeby penetračních testů budeme využívat Linuxovou distribuci Kali, je tudíž nutné ji nejprve stáhnout a nainstalovat. Stáhneme si předpřipravenou Custom edici dostupnou z „https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/#1572305786534-030ce714-cc3b“. Vytvoříme instalační disk pro instalaci na počítač, nebo nainstalujeme jako virtuální stroj pomocí VirtualBoxu, Hyper-v či VMware Workstation. Využijeme pro naše potřeby Oracle VMbox, kde importujeme staženou applianci a následně potvrdíme licenční podmínky. Pro potřeby penetračních testů si vytvoříme nového uživatele v Active Directory (pentest) na našem DC serveru (192.168.230.3), který bude mít pouze uživatelské oprávnění oproti doposud užívanému uživatelskému účtu (nemron1), který je doménový administrátor.



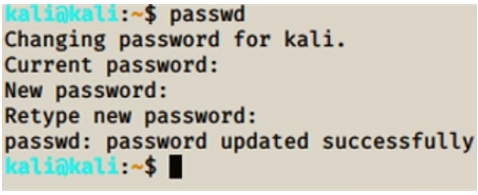
Obrázek 307 - KALI Linux VirtualBox

Dále se přihlásíme defaultním účtem kali. Prvně v terminálu změníme heslo pro náš root účet kali.



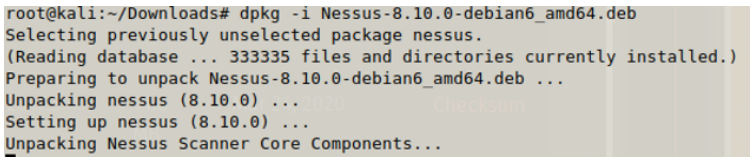
Obrázek 308 - Vytvoření uživatele AD

Obrázek 309 - KALI přihlášení



Obrázek 310 - KALI změna hesla

Pokračujeme instalací softwaru Nessus.



Obrázek 311 - Instalace Nessus

Obrázek 312 - Instalace Nessus č.2

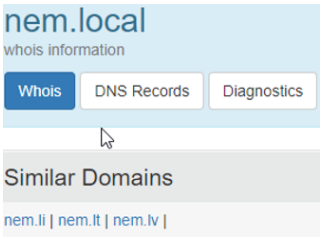
Po nainstalování software Nessus je nutné si vytvořit účet a následně se pomocí něj přihlašovat.

22.1 Reconnaissance (Průzkum)

První částí penetračních testů bude takzvaný průzkum, zde bychom mohli zavést veškeré obvyklé součásti jako fyzický průzkum, nicméně vzhledem k našemu laboratornímu testovacímu prostředí se budeme soustředit pouze na ověření cíle a základní mapování síťového prostředí a infrastruktury.

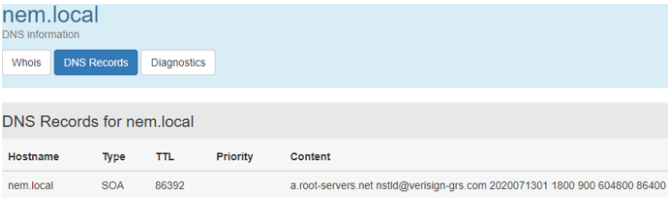
22.1.1 Ověření cíle (domény)

Započneme ověřením, zda jsme schopni získat informace o naší společnosti a doméně v oblasti OSINT (Open Source Intelligence), což jsou vlastně volně dosažitelné informace dostupné na internetu. Podíváme se na web who.is, kde zkusíme vyhledat naši doménu nem.local, kde jsme nenalezli žádné výsledky, neboť doména není oficiálně registrovaná a nevyužívá žádné certifikační autority.



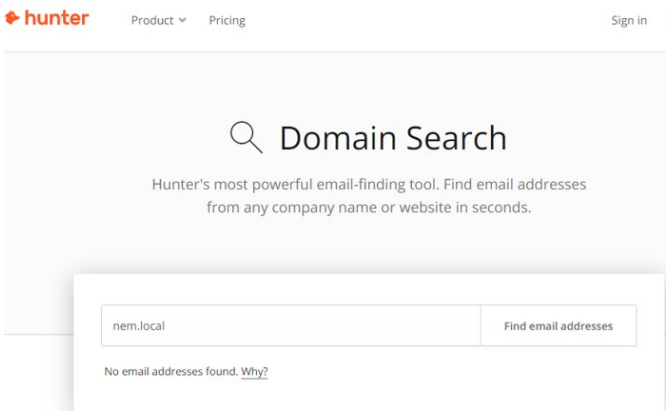
Obrázek 313 - Who.is

Webová databáze nalezla pouze podobné našemu zadání podobné domény nem.li, nem.it, nem.lv. Zároveň byly nalezeny DNS záznamy pro nem.local, nicméně nejedná se o naši doménu.



Obrázek 314 - Who.is č.2

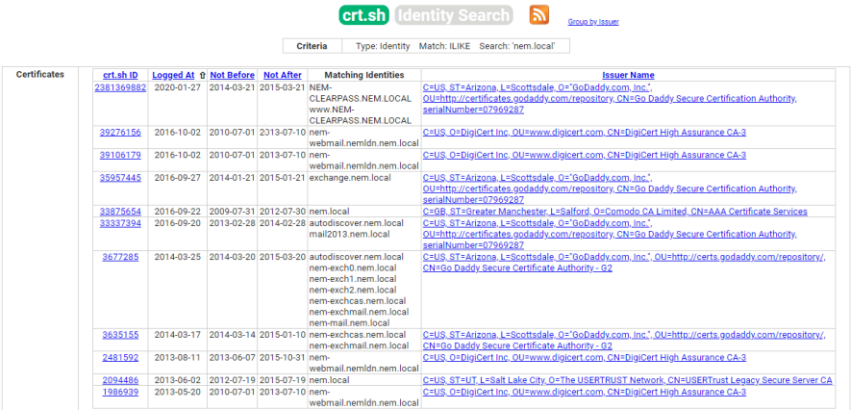
Stejně jako u whois průzkumu využijeme hunter.io, kde se pokusíme nalézt emailové adresy pro naši doménu, nicméně stejně jako v předchozím případě nebude nic nalezeno vzhledem k necertifikované doméně, stejným způsobem využijeme theHarvester přímo v distribuci KALI, pomocí terminálového příkazu theHarvester -d nem.local -l 500, kde „-d“ určuje doménu a „-l“ počet hledání. Nicméně ani v tomto případě nebudou výsledky.



Obrázek 315 - hunter.io

Obrázek 316 - theHarvester

Dále ověříme, že opravdu není k dispozici certifikát pro naši doménu pomocí crt.sh, který nám sice nalezne fungující certifikáty, nicméně všechny odkazující na jiné světové lokality.



Obrázek 317 - crt.sh

22.2 Externí penetrace „veřejné“ adresy

V našem laboratorním prostředí je pro nás veřejnou adresou adresa L3 switche, kterou máme staticky přiřazenou z nadřazeného routeru. První sken provedeme pomocí programu nmap, který nám umožní mimo jiné skenovat porty a provádět ping sweep, zaměříme jej na naší „veřejnou“ adresu což je pro nás adresa L3 switche 192.168.0.110.

```
root@kali:~# nmap -sT -p- -T4 -A -O -sV  192.168.0.110
```

Obrázek 318 - nmap příkaz

Zvolili jsme „-sT“ pro standartní sken, rychlost T4, což je vlastně nejrychlejší možný sken, neboť nás nezajímá, jestli bychom mohli být odhaleni. Dále „-p-“ je značka pro všechny porty, „-sV“ je zjištění verzí služeb na portech a „-A“ a „-O“ jsou parametry pro detekci operačních systémů u hostů. Zvenčí jsme zjistili, že veškeré porty jsou na firewallu filtrovány.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-16 21:40 BST
Stats: 0:15:30 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 70.72% done; ETC: 22:02 (0:06:25 remaining)
Nmap scan report for 192.168.0.110
Host is up (0.0028s latency).
All 65535 scanned ports on 192.168.0.110 are filtered
MAC Address: 64:D1:54:1C:76:07 (Routerboard.com)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   2.84 ms 192.168.0.110

OS and Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1317.41 seconds
root@kali:~#
```

Obrázek 319 - nmap příkaz č.2

Dále ještě otestujeme externí zranitelnosti na naší vnější adrese 192.168.0.110 pomocí „nmap -sT -sV -A -p- --script vuln 192.168.0.110“. Který nám otestuje, jak porty což jsme již udělali v předešlém testu, tak i vulnerability a zkusí nalézt služby, které jsou používány na jednotlivých portech.

```
root@kali:~# nmap -sT -sV -A -p- --script vuln 192.168.0.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-18 13:49 BST
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Sc
an
NSE Timing: About 0.00% done
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.110
Host is up (0.0027s latency).
Not shown: 65533 filtered ports
```

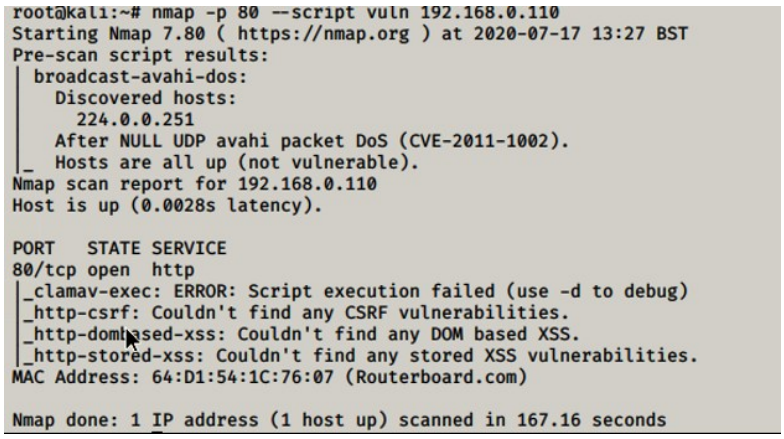
Obrázek 320 - nmap příkaz č.3

```
PORT    STATE SERVICE VERSION
80/tcp  open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp open  https?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
MAC Address: 64:D1:54:1C:76:07 (Routerboard.com)
Warning: OSScan results may be unreliable because we could not find at least
 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incom
plete
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Obrázek 321 - nmap výsledky

22.3 Externí testování webu

První krokem bude i zde nmap, který nám pomůže zjistit porty a dostupné zranitelnosti našeho webového serveru z externího zařízení. Testování provedeme pro porty 80 a 443, dále použijeme možnosti skriptů, které ověří, zda jsou k nalezení známé zranitelnosti.



Obrázek 322 - nmap Webtest

Obrázek 323 - nmap Webtest č.2

Následně použijeme nástroj whatweb, který prozkoumá a uvede technologie i jejich nedostatky, které jsme použili na naší intranetové webové stránce.

```
root@kali:~# whatweb -v https://webnem.nem.local/intranet
WhatWeb report for https://webnem.nem.local/intranet
Status    : 301 Moved Permanently
Title     : Document Moved
IP        : 192.168.250.2
Country   : RESERVED, ZZ

Summary   : RedirectLocation[https://webnem.nem.local/intranet/], Microsoft-
IIS[10.0], HTTPServer[Microsoft-IIS/10.0]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Microsoft-IIS/10.0 (from server string)

[ Microsoft-IIS ]
        Microsoft Internet Information Services (IIS) for Windows
        Server is a flexible, secure and easy-to-manage Web server
        for hosting anything on the Web. From media streaming to
        web application hosting, IIS's scalable and open
        architecture is ready to handle the most demanding tasks.

        Version      : 10.0
        Website     : http://www.iis.net/
```

Obrázek 324 – Whatweb

```
[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://webnem.nem.local/intranet/ (from location)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Content-Type: text/html; charset=UTF-8
        Location: https://webnem.nem.local/intranet/
        Server: Microsoft-IIS/10.0
        Date: Sat, 18 Jul 2020 12:55:09 GMT
        Connection: close
        Content-Length: 157

WhatWeb report for https://webnem.nem.local/intranet/
Status    : 200 OK
Title     : W3.CSS Template
IP        : 192.168.250.2
Country   : RESERVED, ZZ

Summary   : PHP[7.4.1], Email[test@test.com], Microsoft-IIS[10.0], HTTPServe
r[Microsoft-IIS/10.0], HTML5, X-Powered-By[PHP/7.4.1], Script
```

Obrázek 325 - Whatweb č.2

Pomocí příkazu „whatweb -v https://webnem.nem.local/intranet >> ./Desktop/whatweb.txt“, který nám umožní rovnou uložit získaná data do textového souboru, web prozkoumáme.

```
Detected Plugins:
[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
        tags. We match syntactically invalid links containing
        mailto: to catch anti-spam email addresses, eg. bob at
        gmail.com. This uses the simplified email regular
        expression from
        http://www.regular-expressions.info/email.html for valid
        email address matching.

        String       : test@test.com

[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Microsoft-IIS/10.0 (from server string)
```

Obrázek 326 - Whatweb č.3

```
[ Microsoft-IIS ]
        Microsoft Internet Information Services (IIS) for Windows
        Server is a flexible, secure and easy-to-manage Web server
        for hosting anything on the Web. From media streaming to
        web application hosting, IIS's scalable and open
        architecture is ready to handle the most demanding tasks.

        Version      : 10.0
        Website      : http://www.iis.net/

[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 7.4.1
        Google Dorks: (2)
        Website      : http://www.php.net/
```

Obrázek 327 - Whatweb č.4

```
[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.


[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : PHP/7.4.1 (from x-powered-by string)

HTTP Headers:
        HTTP/1.1 200 OK
        Content-Type: text/html; charset=UTF-8
        Server: Microsoft-IIS/10.0
        X-Powered-By: PHP/7.4.1
        Date: Sat, 18 Jul 2020 12:55:15 GMT
        Connection: close
        Content-Length: 12012
```

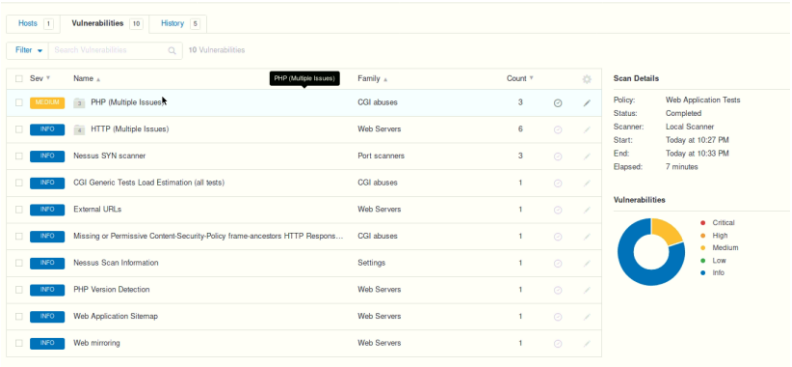
Obrázek 328 - Whatweb č.5

Stejný sken ještě provedeme pomocí nástroje nikto a pokusíme se získat vícero dat. Použijeme proto příkaz „nikto -C -port 80,443 -Tuning x -Cgidirs all -host 192.168.0.110“.

```
root@kali:~# nikto -C -port 80,443 -Tuning x -Cgidirs all -host 192.168.0.11
0
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.110
+ Target Hostname:    192.168.0.110
+ Target Port:        80
+ Start Time:         2020-07-18 14:58:41 (GMT1)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the us
er agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user ag
ent to render the content of the site in a different fashion to the MIME typ
e
+ 26521 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2020-07-18 15:00:43 (GMT1) (122 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Obrázek 329 – nikto

Následně využijeme možností nainstalovaného softwaru Nessus, kde provedeme webscan.



Obrázek 330 - Nessus webscan

22.4 Interní penetrační testy

22.4.1 Zjištění hostů (nslookup, dig, dnsrecon)

Prvně zjistíme dns záznam pro naši lokální doménu a posléze otestujeme DNS zone transfer a zjistíme si informace ohledně DNS serveru domény.

```
root@kali:~# host -t ns nem.local
nem.local name server esx1dc1v.nem.local.
root@kali:~# host -t a nem.local
nem.local has address 192.168.230.3
root@kali:~# host -t mx nem.local
nem.local has no MX record
root@kali:~# host -t aaaa nem.local
nem.local has no AAAA record
root@kali:~# nslookup nem.local
Server:         192.168.230.3
Address:        192.168.230.3#53

Name:   nem.local
Address: 192.168.230.3
```

Obrázek 331- host příkaz

```
root@kali:~# dig axfr nem.local 192.168.230.3

; <<>> DiG 9.16.3-Debian <<>> axfr nem.local 192.168.230.3
;; global options: +cmd
; Transfer failed.
; Transfer failed.
```

Obrázek 332 - dig příkaz

```
root@kali:~# dnsrecon -d nem.local -t axfr
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for nem.local name servers
[*] Resolving SOA Record
[+]      SOA esx1dc1v.nem.local 192.168.230.3
[*] Resolving NS Records
[*] NS Servers found:
[*]     NS esx1dc1v.nem.local 192.168.230.3
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 192.168.230.3
[+] 192.168.230.3 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] Zone transfer error: REFUSED
```

Obrázek 333 - dnsrecon příkaz

Následně vzhledem ke zjištěné adrese 192.168.230.3 zkusíme pingsweep na subnety, abychom zjistili, kde jsou aktivní brány a následně provedeme IP sken daných podsítí pro zjištění spuštěných hostů pomocí příkazu „nmap -sN -v -PE 192.168.*.1“, a následně provedeme stejným způsobem ping objevených používaných subnetů.

```
Nmap scan report for 192.168.200.1
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.200.1 are open|filtered

Nmap scan report for 192.168.215.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.215.1 are open|filtered

Nmap scan report for 192.168.220.1
Host is up (0.00063s latency).
All 1000 scanned ports on 192.168.220.1 are open|filtered

Nmap scan report for 192.168.230.1
Host is up (0.0021s latency).
All 1000 scanned ports on 192.168.230.1 are open|filtered

Nmap scan report for 192.168.250.1
Host is up (0.0050s latency).
All 1000 scanned ports on 192.168.250.1 are open|filtered

Initiating NULL Scan at 21:12
Scanning 192.168.240.1 [1000 ports]
Completed NULL Scan at 21:13, 21.10s elapsed (1000 total ports)
Nmap scan report for 192.168.240.1
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.240.1 are open|filtered
```

Obrázek 334 - nmap scan report

```
root@kali:~# nmap -sL 192.168.200.0/24 | grep nem.local
Nmap scan report for vpn1v.nem.local (192.168.200.2)
```

Obrázek 335 - scan report (200)

```
root@kali:~# nmap -sL 192.168.215.0/24 | grep nem.local
Nmap scan report for backupsv1v.nem.local (192.168.215.2)
```

Obrázek 336 - scan report (215)

```
root@kali:~# nmap -sL 192.168.230.0/24 | grep nem.local
Nmap scan report for esxprt1v.nem.local (192.168.230.4)
Nmap scan report for appsv1v.nem.local (192.168.230.7)
Nmap scan report for wsus1v.nem.local (192.168.230.8)
Nmap scan report for monsv1v.nem.local (192.168.230.10)
Nmap scan report for exsv1v.nem.local (192.168.230.11)
Nmap scan report for mailsv1v.nem.local (192.168.230.12)
Nmap scan report for radsv1v.nem.local (192.168.230.15)
Nmap scan report for fs1v.nem.local (192.168.230.20)
```

Obrázek 337 - scan report (230)

```
root@kali:~# nmap -sL 192.168.240.0/24 | grep nem.local
Nmap scan report for cznnem1.nem.local (192.168.240.6)
```

Obrázek 338 - scan report (240)

```
root@kali:~# nmap -sL 192.168.250.0/24 | grep nem.local
Nmap scan report for webnem.nem.local (192.168.250.2)
```

Obrázek 339 - scan report (250)

22.4.2 Jednotlivé reporty serverů (nmap)

22.4.2.1 Domain controller nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-21 21:36 BST

Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 192.168.240.3
|     Subnet Mask: 255.255.255.0
|     Server Identifier: 192.168.230.3
|     Router: 192.168.240.1
|     Domain Name Server: 192.168.230.3, 192.168.230.3
|     Domain Name: nem.local\x00

Nmap scan report for 192.168.230.3
Host is up (0.0012s latency).
Not shown: 65529 filtered ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.230.3; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.230.3; use dns-nsec3-enum.domains script arg.
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-07-21 20:38:33Z)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
135/tcp  open  msrpc        Microsoft Windows RPC
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: nem.local, Site: Default-First-Site-Name)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
```

Obrázek 340 - DC nmap test

```
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=nem,DC=local
|       ldapServiceName: nem.local:esx1dc1v$@NEM.LOCAL
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2

|       subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=nem,DC=local
|       serverName: CN=ESX1DC1V,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=nem,DC=local
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=nem,DC=local
|       namingContexts: DC=nem,DC=local
|       namingContexts: CN=Configuration,DC=nem,DC=local
|       namingContexts: CN=Schema,CN=Configuration,DC=nem,DC=local
|       namingContexts: DC=DomainDnsZones,DC=nem,DC=local
|       namingContexts: DC=ForestDnsZones,DC=nem,DC=local
|       isSynchronized: TRUE
|       highestCommittedUSN: 125068
|       dsServiceName: CN=NTDS Settings,CN=ESX1DC1V,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=nem,DC=local
|       dnsHostName: esx1dc1v.nem.local
|       defaultNamingContext: DC=nem,DC=local
|       currentTime: 20200721205106.0Z
|_      configurationNamingContext: CN=Configuration,DC=nem,DC=local
|_sslv2-drown:
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: nem.local, Site: Default-First-Site-Name)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)

No OS matches for host
Network Distance: 2 hops
Service Info: Host: ESX1DC1V; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Obrázek 341 - DC nmap test č.2

```
Host script results:
|_dns-brute: Can't guess domain of "192.168.230.3"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
| firewalk:
| HOP  HOST           PROTOCOL  BLOCKED PORTS
|_1    192.168.240.1  tcp       1-10
|_ipidseq: Unknown
|_path-mtu: PMTU == 1500
| qscan:
| PORT  FAMILY  MEAN (us)  STDDEV  LOSS (%)
| 53    0       700.40     126.17  0.0%
| 88    0       704.50     125.18  0.0%
| 135   0       747.90     80.35   0.0%
| 389   0       738.60     128.96  0.0%
| 3268  1       783.80     61.16   0.0%
|_3269  1       784.80     84.57   0.0%


TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.20 ms 192.168.240.1
2   1.48 ms 192.168.230.3

Post-scan script results:
| reverse-index:
|   53/tcp: 192.168.230.3
|   88/tcp: 192.168.230.3
|   135/tcp: 192.168.230.3
|   389/tcp: 192.168.230.3
|   3268/tcp: 192.168.230.3
|_  3269/tcp: 192.168.230.3

Nmap done: 1 IP address (1 host up) scanned in 889.25 seconds
```

Obrázek 342 - DC nmap test č.3

22.4.2.2 File server nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-22 21:54 BST

Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 192.168.240.3
|     Subnet Mask: 255.255.255.0
|     Server Identifier: 192.168.230.3
|     Router: 192.168.240.1
|     Domain Name Server: 192.168.230.3, 192.168.230.3
|_    Domain Name: nem.local\x00

PORT    STATE SERVICE       VERSION
53/tcp  open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?

Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=265 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -43s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-07-23T09:43:02
|_  start_date: N/A

TRACEROUTE (using port 445/tcp)
HOP RTT     ADDRESS
1   1.21 ms 192.168.240.1
2   1.55 ms 192.168.230.20

Nmap done: 1 IP address (0 hosts up) scanned in 43.92 seconds
```

Obrázek 343 - DC nmap test č.4

22.4.2.3 Application server nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-23 11:22 BST

PORT    STATE SERVICE  VERSION
53/tcp  open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp  open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
443/tcp open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
| ssl-cert: Subject: commonName=appsv1v.nem.local
| Subject Alternative Name: DNS:appsv1v.nem.local
| Issuer: commonName=appsv1v.nem.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-07-16T13:19:27
| Not valid after:  2021-07-16T00:00:00
| MD5:   6570 b687 951c 4113 cf7c 70de 18e5 7ce4
|_SHA-1: 2b11 c7e4 eaa7 a2e6 ae0f 5bb0 3bff 4e38 2138 cf29
|_ssl-date: 2020-07-23T10:24:56+00:00; -43s from scanner time.

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -43s

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.02 ms 192.168.240.1
2   1.11 ms 192.168.230.7
```

Obrázek 344 - Aplikační server nmap test

```
PORT    STATE SERVICE
53/tcp  open  domain
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.230.7; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.230.7; use dns-nsec3-enum.domains script arg.
80/tcp  open  http
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-brute:
|_  Path "/" does not require authentication
|_http-chrono: Request times for /; avg: 178.80ms; min: 176.50ms; max: 181.01ms
|_http-comments-displayer: Couldn't find any comments.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-date: Thu, 23 Jul 2020 11:27:32 GMT; -43s from local time.
|_http-devframework: Couldn't determine the underlying framework or CMS.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=192.168.230.7
|   Found the following error pages:
|
|   Error Code: 404
|_      https://192.168.230.7:443/
|_http-feed: Couldn't find any feeds.
|_http-fetch: Please enter the complete path of the directory to save data in.
| http-headers:
|   Content-Type: text/html; charset=us-ascii
|   Server: Microsoft-HTTPAPI/2.0
|   Date: Thu, 23 Jul 2020 11:57:38 GMT
|   Connection: close
|   Content-Length: 315
|
|_  (Request type: GET)
|_http-malware-host: Host appears to be clean
|_http-mobileversion-checker: No mobile version detected.
|_http-referer-checker: Couldn't find any cross-domain scripts.
| http-security-headers:
|   Strict_Transport_Security:
|_    HSTS not configured in HTTPS Server
|_http-server-header: Microsoft-HTTPAPI/2.0
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_
```

Obrázek 345 - Aplikační server nmap test č.2

```
|_http-slowloris: false
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Not Found
| http-useragent-tester:
|   Status for browser useragent: 404
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
| http-vhosts:
|_127 names had status 404
|_http-xssed: No previously reported XSS vuln.
| ssl-cert: Subject: commonName=appsv1v.nem.local
| Subject Alternative Name: DNS:appsv1v.nem.local
| Issuer: commonName=appsv1v.nem.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-07-16T13:19:27
| Not valid after:  2021-07-16T00:00:00
| MD5:   6570 b687 951c 4113 cf7c 70de 18e5 7ce4
|_SHA-1: 2b11 c7e4 eaa7 a2e6 ae0f 5bb0 3bff 4e38 2138 cf29
|_ssl-date: 2020-07-23T11:59:48+00:00; -43s from scanner time.
```

Obrázek 346 - Aplikační server nmap test č.3

```
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|_  least strength: C
|_sslv2-drown:
| tls-alpn:
|_  http/1.1

Nmap done: 1 IP address (1 host up) scanned in 3792.23 seconds
```

Obrázek 347 - Aplikační server nmap test č.4

22.4.2.4 Backup server nmap scan

```
Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 192.168.240.3
|     Subnet Mask: 255.255.255.0
|     Server Identifier: 192.168.230.3
|     Router: 192.168.240.1
|     Domain Name Server: 192.168.230.3, 192.168.230.3
|_    Domain Name: nem.local\x00

Nmap scan report for 192.168.215.2
Host is up (0.00088s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.215.2; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.215.2; use dns-nsec3-enum.domains script arg.
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
6160/tcp  open  msrpc   Microsoft Windows RPC
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
11731/tcp open  msrpc   Microsoft Windows RPC
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
|_dns-brute: Can't guess domain of "192.168.215.2"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
|_firewalk: None found
|_ipidseq: Incremental!
|_path-mtu: PMTU == 1500
| qscan:
| PORT   FAMILY  MEAN (us)  STDDEV  LOSS (%)
| 53     0       818.80     88.83   0.0%
| 6160   0       912.20     225.69  0.0%
|_11731  1       922.00     102.53  0.0%

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.16 ms 192.168.215.2
 Post-scan script results:
| reverse-index:
|   53/tcp: 192.168.215.2
|   6160/tcp: 192.168.215.2
|_  11731/tcp: 192.168.215.2
Nmap done: 1 IP address (1 host up) scanned in 876.62 seconds
```

Obrázek 348 - Backup nmap test

22.4.2.5 Exchange server nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-22 19:49 BST

Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 192.168.240.3
|     Subnet Mask: 255.255.255.0
|     Server Identifier: 192.168.230.3
|     Router: 192.168.240.1
|     Domain Name Server: 192.168.230.3, 192.168.230.3
|_    Domain Name: nem.local\x00

Nmap scan report for 192.168.230.11
Host is up (0.00079s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.230.11; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.230.11; use dns-nsec3-enum.domains script arg.
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind

Network Distance: 1 hop
Host script results:
|_dns-brute: Can't guess domain of "192.168.230.11"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
|_firewalk: None found
|_ipidseq: Incremental!
|_path-mtu: PMTU == 1500

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.22 ms 192.168.230.11

Post-scan script results:
| reverse-index:
|_  53/tcp: 192.168.230.11
Nmap done: 1 IP address (1 host up) scanned in 877.10 seconds
```

Obrázek 349 - Exchange nmap test

22.4.2.6 Webserver nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-21 19:23 BST

Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).

Nmap scan report for 192.168.250.2
Host is up (0.00088s latency).
Not shown: 65532 filtered ports
PORT    STATE SERVICE VERSION
53/tcp  open  domain?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.250.2; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.250.2; use dns-nsec3-enum.domains script arg.
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp  open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-brute:
|_  Path "/" does not require authentication
|_http-chrono: Request times for /; avg: 152.57ms; min: 151.69ms; max: 154.06ms
|_http-comments-displayer: Couldn't find any comments.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-date: Tue, 21 Jul 2020 18:57:20 GMT; -43s from local time.
|_http-devframework: Couldn't determine the underlying framework or CMS.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=192.168.250.2
|   Found the following error pages:
|
|   Error Code: 404
|_      http://192.168.250.2:80/
|_http-feed: Couldn't find any feeds.
|_http-fetch: Please enter the complete path of the directory to save data in.
| http-headers:
|   Content-Type: text/html; charset=us-ascii
|   Server: Microsoft-HTTPAPI/2.0
|   Date: Tue, 21 Jul 2020 18:57:31 GMT
|   Connection: close
|   Content-Length: 315
|
```

Obrázek 350 - Webserver nmap test

```
|_  (Request type: GET)
|_http-mobileversion-checker: No mobile version detected.
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-security-headers:
|_http-server-header: Microsoft-HTTPAPI/2.0
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_
|_http-slowloris: false
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Not Found
| http-useragent-tester:
|   Status for browser useragent: 404
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
```

Obrázek 351 - Web server nmap test č.2

```
| http-vhosts:
|_127 names had status 404
|_http-xssed: No previously reported XSS vuln.
443/tcp open  https?
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-brute:
|_  Path "/" does not require authentication
|_http-chrono: Request times for /; avg: 8175.14ms; min: 8165.52ms; max: 8179.79ms
|_http-comments-displayer: Couldn't find any comments.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-devframework: Couldn't determine the underlying framework or CMS.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-errors: ERROR: Script execution failed (use -d to debug)
|_http-feed: Couldn't find any feeds.
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-mobileversion-checker: No mobile version detected.
|_http-referer-checker: Couldn't find any cross-domain scripts.
| http-security-headers:
|   Strict_Transport_Security:
|_    HSTS not configured in HTTPS Server
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_
|_http-slowloris: false
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-useragent-tester:
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
```

Obrázek 352 - Web server nmap test č.3

```
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -43s
|_dns-brute: Can't guess domain of "192.168.250.2"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
|_firewalk: None found
|_ipidseq: Incremental!
|_path-mtu: PMTU == 1500
| qscan:
| PORT  FAMILY  MEAN (us)  STDDEV  LOSS (%)
| 53    0       820.60     117.14  0.0%
| 80    0       751.30     159.89  0.0%
|_443   0       704.80     184.47  0.0%
| traceroute-geolocation:
|   HOP  RTT   ADDRESS        GEOLOCATION
|_  1    1.03  192.168.250.2  - ,-

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.03 ms 192.168.250.2

Post-scan script results:
| reverse-index:
|   53/tcp: 192.168.250.2
|   80/tcp: 192.168.250.2
|_  443/tcp: 192.168.250.2

Nmap done: 1 IP address (1 host up) scanned in 3946.82 seconds
```

Obrázek 353 - Web server nmap test č.4

22.4.2.7 Monitoring server nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-22 21:30 BST

Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).

Nmap scan report for 192.168.230.10
Host is up (0.00080s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.230.10; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.230.10; use dns-nsec3-enum.domains script arg.
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind

Network Distance: 1 hop

Host script results:
|_dns-brute: Can't guess domain of "192.168.230.10"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
|_firewalk: None found
|_ipidseq: Incremental!
|_path-mtu: PMTU == 1500
| traceroute-geolocation:
|   HOP  RTT   ADDRESS        GEOLOCATION
|_  1    1.02  192.168.230.10  - ,-
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.02 ms 192.168.230.10

Post-scan script results:
| reverse-index:
|_  53/tcp: 192.168.230.10
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 876.11 seconds
```

Obrázek 354 - Monitoring server nmap test

22.4.2.8 Print server nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-22 21:12 BST

Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).

Nmap scan report for 192.168.230.4
Host is up (0.00084s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.230.4; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.230.4; use dns-nsec3-enum.domains script arg.
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind

Network Distance: 1 hop
Host script results:
|_dns-brute: Can't guess domain of "192.168.230.4"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
|_firewalk: None found
|_ipidseq: Incremental!
|_path-mtu: PMTU == 1500
| traceroute-geolocation:
|   HOP  RTT   ADDRESS        GEOLOCATION
|_  1    1.13  192.168.230.4  - ,-
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.13 ms 192.168.230.4

Post-scan script results:
| reverse-index:
|_  53/tcp: 192.168.230.4
Nmap done: 1 IP address (1 host up) scanned in 876.15 seconds
```

Obrázek 355 - Print server nmap test

22.4.2.9 Radius server nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-22 20:55 BST
Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).

Nmap scan report for 192.168.230.15
Host is up (0.00079s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.230.15; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.230.15; use dns-nsec3-enum.domains script arg.
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind

Network Distance: 1 hop
Host script results:
|_dns-brute: Can't guess domain of "192.168.230.15"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
|_firewalk: None found
|_ipidseq: Incremental!
|_path-mtu: PMTU == 1500
| traceroute-geolocation:
|   HOP  RTT   ADDRESS         GEOLOCATION
|_  1    1.18  192.168.230.15  - ,-
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.18 ms 192.168.230.15

Post-scan script results:
| reverse-index:
|_  53/tcp: 192.168.230.15
Nmap done: 1 IP address (1 host up) scanned in 875.98 seconds
```

Obrázek 356 - Radius server nmap test

22.4.2.10 VPN server nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-21 15:39 BST

Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).

Nmap scan report for 192.168.200.2
Host is up (0.00082s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.200.2; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.200.2; use dns-nsec3-enum.domains script arg.
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind

Network Distance: 1 hop

Host script results:
|_dns-brute: Can't guess domain of "192.168.200.2"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
|_firewalk: None found
|_ipidseq: Incremental!
|_path-mtu: PMTU == 1500


TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.17 ms 192.168.200.2

Post-scan script results:
| reverse-index:
|_  53/tcp: 192.168.200.2
Nmap done: 1 IP address (1 host up) scanned in 877.02 seconds
```

Obrázek 357 - VPN server nmap test

22.4.2.11 SMTP server nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-22 20:12 BST

Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).

Nmap scan report for 192.168.230.12
Host is up (0.00076s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.230.12; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.230.12; use dns-nsec3-enum.domains script arg.
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind

Network Distance: 1 hop
Host script results:
|_dns-brute: Can't guess domain of "192.168.230.12"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
|_firewalk: None found
|_ipidseq: Incremental!
|_path-mtu: PMTU == 1500
| traceroute-geolocation:
|   HOP  RTT   ADDRESS        GEOLOCATION
|_  1    1.22  192.168.230.12  - ,-
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.22 ms 192.168.230.12

Post-scan script results:
| reverse-index:
|_  53/tcp: 192.168.230.12
Nmap done: 1 IP address (1 host up) scanned in 876.12 seconds
```

Obrázek 358 - SMTP server nmap test

22.4.2.12 Wsus server nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-21 21:59 BST

Pre-scan script results:
| broadcast-avahi-dos:
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).

Nmap scan report for 192.168.230.8
Host is up (0.00082s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_dns-fuzz: The server seems impervious to our assault.
|_dns-nsec-enum: Can't determine domain for host 192.168.230.8; use dns-nsec-enum.domains script arg.
|_dns-nsec3-enum: Can't determine domain for host 192.168.230.8; use dns-nsec3-enum.domains script arg.
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind

Network Distance: 1 hop
Host script results:
|_dns-brute: Can't guess domain of "192.168.230.8"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
|_firewalk: None found
|_ipidseq: Incremental!
|_path-mtu: PMTU == 1500
| traceroute-geolocation:
|   HOP  RTT   ADDRESS       GEOLOCATION
|_  1    1.19  192.168.230.8  - ,-
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   1.19 ms 192.168.230.8

Post-scan script results:
| reverse-index:
|_  53/tcp: 192.168.230.8
Nmap done: 1 IP address (1 host up) scanned in 876.06 seconds
```

Obrázek 359 - WSUS server nmap test

22.4.3 HYDRA

Pomocí tohoto testovacího nástroje otestujeme brute-force útoky na hesla a zároveň i dictionary útoky. Nejprve zkusíme útok na službu vzdáleného přístupu, neboť to je jedna z mála služeb povolených v naší síti, nicméně to bude neúspěšné, neboť RDP je povolenou pouze z administrátorského počítače. Následně zkusíme zdolat heslo u uživatele pentest v rámci rdp a přihlášení na náš DC server příkazem „hydra -l pentest -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 6 rdp://192.168.230.3“. Použijeme password list unix_passwords.txt, který je již předem dostupný v rámci KALI Linux distribuce. Nicméně odpovědí bude, že spojení nebylo úspěšné, neboť nám rdp blokuje firewall. Pro naše účely jej povolíme na webserver a posléze otestujeme prolomitelnost hesla při připojení přes RDP na 192.168.250.2 (pomocí jiného wordlistu), nicméně zde hraje roli omezení globální politikou, kdy vyzkoušíme pět hesel a následně je účet uzamčen.

```
root@kali:~# hydra -l pentest -P /usr/share/wordlists/metasploit/unix_passwords.txt -
t 6 rdp://192.168.230.3
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret servi
ce organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-18 15:52:36
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce t
he number of parallel connections and -W 1 or -W 3 to wait between connection to allo
w the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1009 login tries (l:1/p:1009), ~253
 tries per task
[DATA] attacking rdp://192.168.230.3:3389/
[ERROR] freerdp: The connection failed to establish.
```

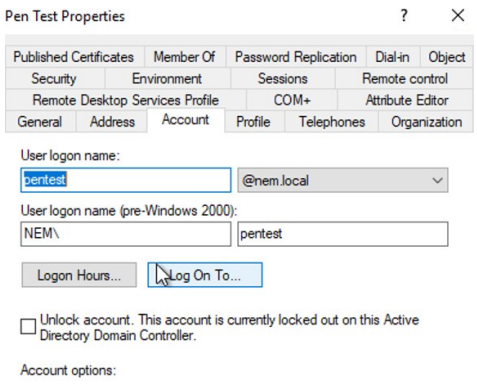
Obrázek 360 - Hydra test

```
root@kali:~# hydra -f  -l pentest -P /usr/share/wordlists/rockyou.txt rdp://
192.168.250.2
```

Obrázek 361- Hydra vůči RDP

```
[DATA] attacking rdp://192.168.250.2:3389/
[STATUS] 378.00 tries/min, 378 tries in 00:01h, 14344028 to do in 632:28h, 4
 active
```

Obrázek 362 - Hydra vůči RDP č.2



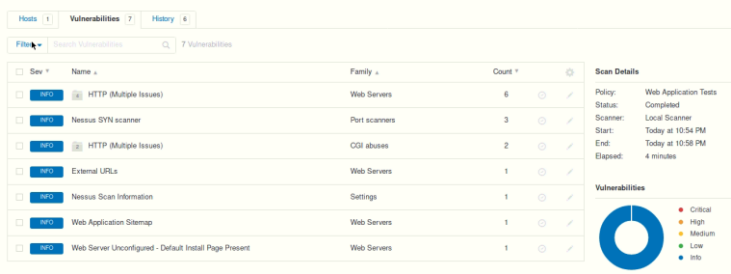
Obrázek 363 - Zamčený AD účet

```
root@kali:~# hydra -l pentest -P /usr/share/wordlists/metasploit/unix_passwords.txt l
dap2://192.168.240.2
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret servi
ce organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-18 20:56:30
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting
)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1009 login tries (l:1/p:1009), ~6
4 tries per task
[DATA] attacking ldap2://192.168.240.2:389/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 993 to do in 00:32h, 16 active
[STATUS] 32.00 tries/min, 96 tries in 00:03h, 946 to do in 00:30h, 16 active
[STATUS] 32.00 tries/min, 224 tries in 00:07h, 818 to do in 00:26h, 16 active
[STATUS] 30.67 tries/min, 368 tries in 00:12h, 674 to do in 00:22h, 16 active
[STATUS] 30.12 tries/min, 512 tries in 00:17h, 530 to do in 00:18h, 16 active
[STATUS] 30.41 tries/min, 669 tries in 00:22h, 373 to do in 00:13h, 16 active
[STATUS] 30.22 tries/min, 816 tries in 00:27h, 226 to do in 00:08h, 16 active
[STATUS] 30.00 tries/min, 960 tries in 00:32h, 82 to do in 00:03h, 16 active
[STATUS] 30.06 tries/min, 992 tries in 00:33h, 50 to do in 00:02h, 16 active
[STATUS] 30.12 tries/min, 1024 tries in 00:34h, 18 to do in 00:01h, 16 active
[STATUS] 29.77 tries/min, 1042 tries in 00:35h, 1 to do in 00:01h, 2 active
1 of 1 target completed, 0 valid passwords found
```

Obrázek 364 - Hydra výsledek

22.4.4 Zkoumání aplikačního serveru

Stejně jako jsme externě otestovali webový server, tak pomocí nessus softwaru zkontrolujeme náš aplikační server.



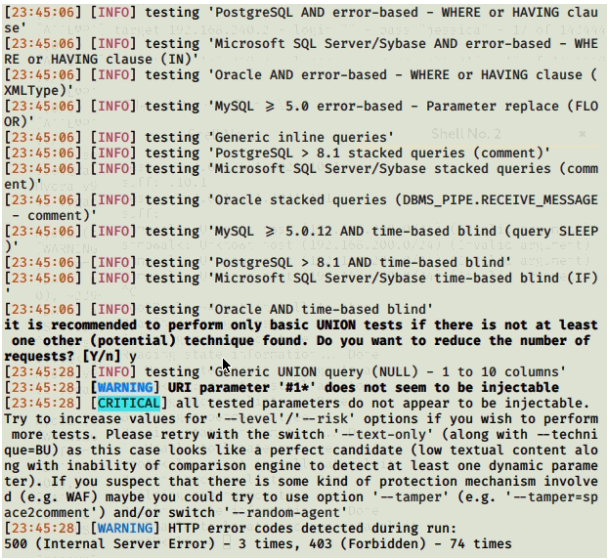
Obrázek 365 - Nessus aplikační server test

22.4.5 SQLMAP

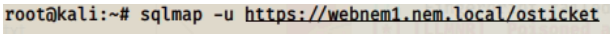
Zde vyzkoušíme SQL injection útok vůči našemu webovému a následně i aplikačnímu serveru.

```
root@kali:~# sqlmap -u http://webnem.nem.local/intranet -dbs

                        {1.4.6#stable}
                        http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mu
tual consent is illegal. It is the end user's responsibility to obey all app
licable local, state and federal laws. Developers assume no liability and ar
e not responsible for any misuse or damage caused by this program

[*] starting @ 23:44:59 /2020-07-18/

[23:44:59] [WARNING] you've provided target URL without any GET parameters (
e.g. 'http://www.site.com/article.php?id=1') and without providing any POST
parameters through option '--data'
y
[23:45:05] [INFO] testing connection to the target URL
[23:45:05] [WARNING] the web server responded with an HTTP error code (500)
which could interfere with the results of the tests
[23:45:05] [INFO] checking if the target is protected by some kind of WAF/IP
S
[23:45:05] [INFO] testing if the target URL content is stable
[23:45:06] [INFO] target URL content is stable
[23:45:06] [INFO] testing if URI parameter '#1*' is dynamic
[23:45:06] [WARNING] potential permission problems detected ('Access is deni
ed')
[23:45:06] [INFO] URI parameter '#1*' appears to be dynamic
[23:45:06] [WARNING] heuristic (basic) test shows that URI parameter '#1*' m
ight not be injectable
[23:45:06] [INFO] testing for SQL injection on URI parameter '#1*'
[23:45:06] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:45:06] [INFO] testing 'Boolean-based blind - Parameter replace (original
 value)'
[23:45:06] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORD
ER BY or GROUP BY clause (FLOOR)'
```

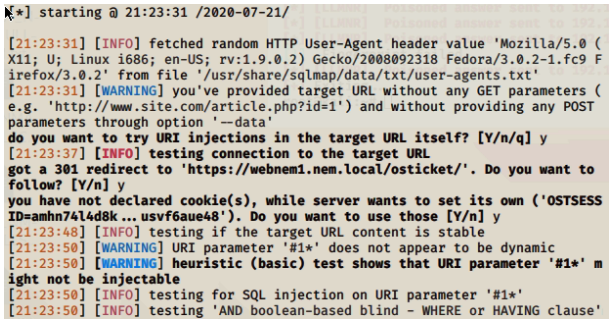
Obrázek 366 - SQLmap vůči webserveru



Obrázek 367 - SQLmap vůči webserveru č.2



Obrázek 368 - SQLmap vůči aplikačnímu serveru



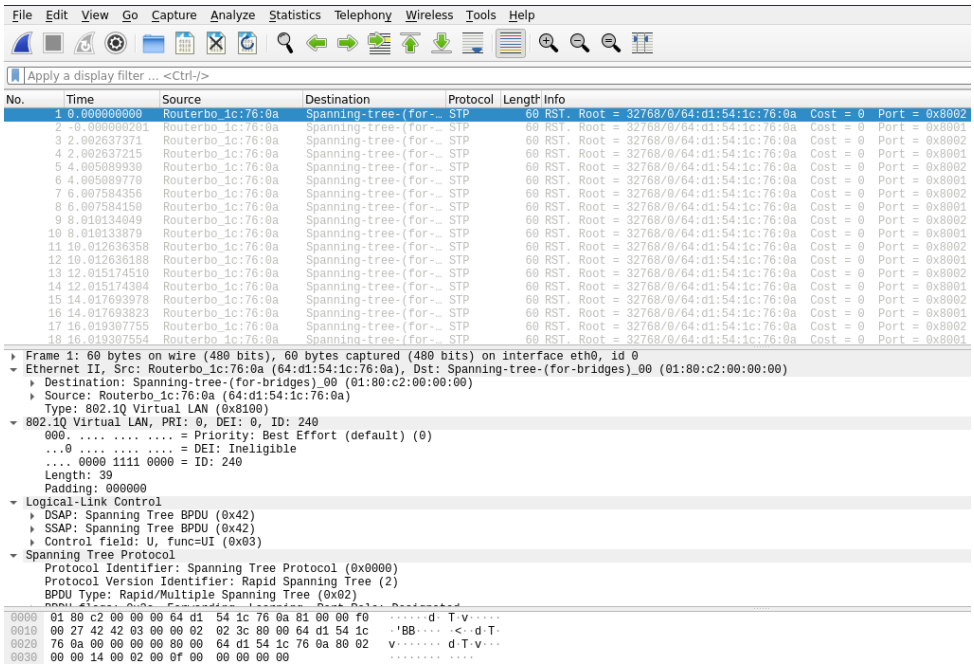
Obrázek 369 - SQLmap vůči aplikačnímu serveru č.2

```
[21:23:50] [INFO] testing 'Boolean-based blind - Parameter replace (original
 value)'
[21:23:50] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORD
ER BY or GROUP BY clause (FLOOR)'
[21:23:50] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clau
se'
[21:23:50] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHE
RE or HAVING clause (IN)'
[21:23:50] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (
XMLType)'
[21:23:50] [INFO] testing 'MySQL ≥ 5.0 error-based - Parameter replace (FLO
OR)'
[21:23:50] [INFO] testing 'Generic inline queries'
[21:23:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[21:23:50] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comm
ent)'
[21:23:51] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE
 - comment)'
[21:23:51] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP
)'
[21:23:51] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[21:23:51] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)
'
[21:23:51] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least
 one other (potential) technique found. Do you want to reduce the number of
requests? [Y/n] y
[21:23:59] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[21:23:59] [WARNING] URI parameter '#1*' does not seem to be injectable
[21:23:59] [CRITICAL] all tested parameters do not appear to be injectable.
Try to increase values for '--level'/'--risk' options if you wish to perform
 more tests. If you suspect that there is some kind of protection mechanism
involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--ta
mper=space2comment')
[21:23:59] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 73 times

[*] ending @ 21:23:59 /2020-07-21/
```

Obrázek 370 - SQLmap vůči aplikačnímu serveru č.3

22.4.6 Wireshark

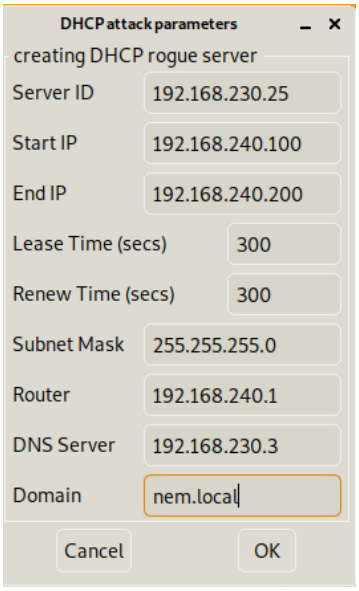
Pomocí wiresharku z našeho Kali Linux systému otestujeme, zda budeme schopni „vyčmuchat“ informace, které by dále mohly být použity k útoku na naši infrastrukturu. Z testu jsme nezískali žádné cenné informace pro další možné útoky. Nicméně tento test by byl vhodnější v chodu systému s několika desítkami uživatelů, kdy je vyšší pravděpodobnost cenného nálezu.



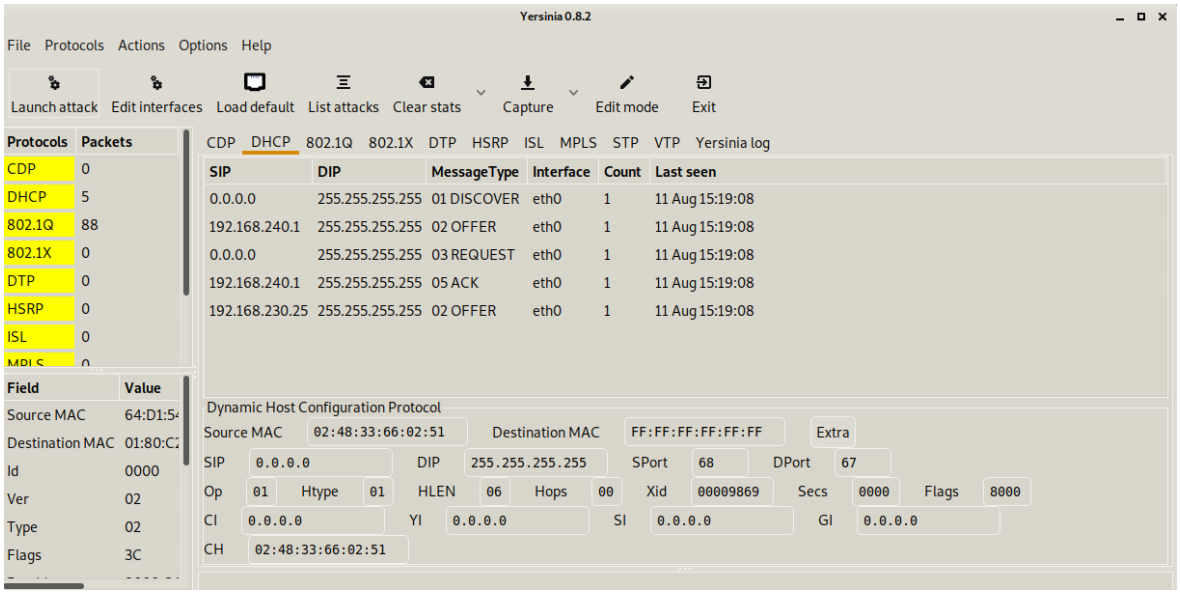
Obrázek 371 – Wireshark

22.4.7 Yersinia

Pomocí softwaru Yersinia vystavíme pro ukázku falešný DHCP server, který nastavíme a následně spustíme test. IP adresu serveru zvolíme 192.168.230.25, masku 255.255.255.0 a bránu 192.168.230.1. Nastavíme adresní rozsah a doménu nem.local. Následně test spustíme. Z testu lze vyčíst, že server adresu nabídl nicméně nebyla přijata, tudíž byl test neúspěšný.



Obrázek 372 – Yersinia



Obrázek 373 - Yersinia test

ZÁVĚR

V rámci diplomové práce jsme vytvořili funkční infrastrukturu pro firemní prostředí, která je obecně aplikovatelná a modifikovatelná dle potřeb konkrétní společnosti. Prvně jsme vytvořili návrh síťové infrastruktury a začali s tvorbou síťového prostředí. Prvním krokem bylo nastavení L3 routeru a následně aktivace ESXi hostitele, kde byly posléze vytvořeny všechny naše virtuální stroje. Dalšími kroky tvořily instalace a nastavení doménového kontroleru a zprostředkovatelů DNS a DHCP služeb. Postupně jsme doplňovaly serverové pole dalšími servery, které nám nabízejí další služby. Posléze jsme započali prvními kroky pro zabezpečení zavedených strojů pomocí doménových politik. Dalším krokem byla konstrukce firewallu, který náš systém ochrání vůči vnějším i vnitřním útokům. Následně jsme pomocí penetračních testů ověřili bezpečnost námi vytvořené síťové i serverové struktury a firewallu. V rámci našich penetračních testů se nám z externí IP adresy (vnější sítě) nepodařilo zjistit téměř nic, kromě otevřených portů 80,443, které nicméně byly stejně filtrované. Dále pak z vnitřní sítě byly provedeny SQL injection, password brute-force a další skeny. Nicméně ani tyto neodhalily krom portů potřebných na určitých serverech zásadní možnosti průniku útočníka a byly tak v konečném slova smyslu neúspěšné. Tato diplomová práce může posloužit pro jako návod pro účely vytvoření firemní sítě. Praktická část práce je vedena obecně, a tudíž lze tvořenou infrastrukturu modifikovat. I přes skutečnost, že byla práce provedena v laboratorním prostředí, byla její funkčnost ověřena v rámci možností ESXi hosta a testy byly provedeny důkladně avšak pouze v modré zóně, což znamená, že jsme se nepokoušeli o malware útoky či využití známých chyb v systémech Windows či jejich podsystémech a jejich službách.

SEZNAM POUŽITÉ LITERATURY

[1] What Is the Difference Between Physical Servers and VMs?. VM Backup | VMware Backup | Hyper-V Backup | EC2 Backup - NAKIVO [online]. Copyright ©2020 NAKIVO, Inc. All Rights Reserved [cit. 26. 07. 2020]. Dostupné z: https://www.nakivo.com/blog/physical-servers-vs-virtual-machines-key-differences-similarities/

[2] HP ProLiant DL360 Generation 7 (QuickSpecs/c04284501.pdf). [online]. Dostupné z: https://h20195.www2.hpe.com/v2/Getdocument.aspx?docname=c04284501

[3] Wireshark · Go Deep.. Wireshark · Go Deep. [online]. Dostupné z: https://www.wireshark.org/

[4] What is vSphere 7? | Server Virtualization Software | VMware. VMware – Official Site [online]. Copyright © 2020 VMware, Inc [cit. 26. 07. 2020]. Dostupné z: https://www.vmware.com/products/vsphere.html

[5] MikroTik Routers and Wireless - Products: RB2011UiAS-IN. MikroTik Routers and Wireless [online]. Dostupné z: https://mikrotik.com/product/RB2011UiAS-IN

[6] osTicket | Support Ticketing System. osTicket | Support Ticketing System [online]. Copyright © 2020. All Rights Reserved. A Product Of [cit. 26. 07. 2020]. Dostupné z: https://osticket.com/

[7] Veeam is the global leader in Backup that delivers Cloud Data Management. Veeam is the global leader in Backup that delivers Cloud Data Management [online]. Copyright ©2020 Veeam [cit. 26. 07. 2020]. Dostupné z: https://www.veeam.com/

[8] Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution [online]. Copyright © 2001 [cit. 26. 07. 2020]. Dostupné z: https://www.zabbix.com/

[9] VPN Software Solutions & Services For Business | OpenVPN. VPN Software Solutions & Services For Business | OpenVPN [online]. Copyright © 2020 OpenVPN Inc. [cit. 26. 07. 2020]. Dostupné z: https://openvpn.net/

[10] Configuring RADIUS Authentication in Windows Server 2016. Vembu: Simplifying Data Protection for Virtual & Physical Data Centers [online]. Dostupné z: https://www.vembu.com/blog/configuring-radius-authentication-in-windows-server-2016-ad-sonicwall/

[11] Windows Server Update Services – Wikipedie. [online]. Dostupné z: https://cs.wikipedia.org/wiki/Windows_Server_Update_Services

[12] What is BYOD (bring your own device)? - Definition from WhatIs.com. Computer Glossary, Computer Terms - Technology Definitions and Cheat Sheets from WhatIs.com - The Tech Dictionary and IT Encyclopedia [online]. Dostupné z: https://whatis.techtarget.com/definition/BYOD-bring-your-own-device

[13] KIM, Peter. Hacking: praktický průvodce penetračním testováním. Přeložil Jan POKORNÝ. Brno: Zoner Press, 2015. Encyklopedie Zoner Press. ISBN 978-80-7413-313-8

[14] VMware vSphere Documentation. VMware Docs Home [online]. Copyright © [cit. 27. 07. 2020]. Dostupné z: https://docs.vmware.com/en/VMware-vSphere/index.html

[15] Manual:TOC - MikroTik Wiki. [online]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:TOC

[16] Manual:Securing Your Router - MikroTik Wiki. [online]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router

[17] Thomas, O. Windows server 2019 inside out. Redmond, WA: Microsoft Press, 2020.

[18] Reference manual for OpenVPN 2.4 | OpenVPN. VPN Software Solutions & Services For Business | OpenVPN [online]. Copyright © 2020 OpenVPN Inc. [cit. 27.07.2020]. Dostupné z: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/

[19] Getting Started - Quick Start Guide for VMware vSphere. 301 Moved Permanently [online]. Copyright © [cit. 27.07.2020]. Dostupné z: https://helpcenter.veeam.com/docs/backup/qsg_vsphere/getting_started.html?ver=100

[20] osTicket Documentation Release 1.14.1, 2020. [online] Enhancesoft. Dostupné z: https://rtd.enhancesoft.com/media/pdf/docs/latest/docs.pdf

[21] Zabbix Manual [Zabbix Documentation 5.0]. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution [online]. Copyright © 2001 [cit. 27.07.2020]. Dostupné z: https://www.zabbix.com/documentation/current/manual

[22] KRAUSE, J. (2018). MASTERING WINDOWS GROUP POLICY: Improve and reimagine your organization's security, network ..., and server management with gpmc and powershell. Place of publication not identified: PACKT Publishing Limited.

[23] Windows Account Policies. Randy Franklin Smith's Ultimate Windows Security [online]. Copyright ©2006 [cit. 28.07.2020]. Dostupné z: https://www.ultimatewindowssecurity.com/wiki/page.aspx?spid=AccountPolicies

[24] W3.CSS Templates. W3Schools Online Web Tutorials [online]. Dostupné z: https://www.w3schools.com/w3css/w3css_templates.asp

[25] BROOKS, R. R. Introduction to computer and network security: navigating shades of gray. Boca Raton: CRC Press, c2014. ISBN 978-1-4398-6071-7.

[26] SELECKÝ, Matúš. Penetrační testy a exploitace. Brno: Computer Press, 2012. ISBN 978-80-251-3752-9.

[27] Sys Admin: the journal for UNIX and Linux systems administrators. San Francisco: CMP Media LLC. ISSN 1061-2688.

[28] BINNIE, Chris. Linux Server security: hack and defend. Indianapolis, Indiana: Wiley, [2016].

SEZNAM OBRÁZKŮ