



Střední škola informatiky a služeb  
Dvůr Králové nad Labem

18-20-M/01 Informační technologie

# Závěrečná práce – „Nemocnice“

Tomáš Batelka, 3.I

Školní rok 2019/2020

## Obsah

1.	Úvod.....	1
2.	Instalace.....	2
2.1.	Windows Server 2019.....	2
2.1.1.	Vytvoření virtuálního stroje.....	2
2.1.2.	Instalace systému.....	2
2.1.3.	Změna hostname.....	2
2.1.4.	Konfigurace sítě.....	3
2.2.	Windows 10.....	3
2.2.1.	Vytvoření virtuálního stroje.....	3
2.2.2.	Instalace systému.....	4
2.2.3.	Změna hostname.....	4
3.	Instalace a konfigurace rolí.....	5
3.1.	Instalace.....	5
3.2.	DHCP Server.....	5
3.2.1.	Server.....	5
3.2.2.	Klient.....	6
3.3.	Řadič domény.....	7
3.3.1.	Server.....	7
3.3.2.	Klient.....	7
4.	Konfigurace Active Directory.....	8
4.1.	Organizační jednotky.....	8
4.2.	Domovský adresář.....	8
4.3.	Skupiny.....	8
4.4.	Uživatelé.....	9
5.	Vytvoření a mapování jednotek.....	10
5.1.	Sdílení adresářů.....	10
5.2.	Vytvoření objektu skupinové politiky (GPO).....	10
5.3.	Test.....	11
6.	Nastavení politik.....	12
6.1.	Konfigurace.....	12
6.2.	Test.....	12
7.	Mail.....	13
7.1.	Kerio MailServer.....	13
7.1.1.	Instalace.....	13

7.1.2.	Konfigurace .....	13
7.1.3.	Firewall .....	14
7.2.	Mozilla Thunderbird klient .....	15
7.2.1.	Instalace .....	15
7.2.2.	Konfigurace .....	15
7.2.3.	Test .....	15
8.	FTP .....	16
8.1.	FTP server .....	16
8.1.1.	Instalace .....	16
8.1.2.	Konfigurace .....	16
8.1.3.	Firewall .....	16
8.2.	FTP klient .....	16
8.2.1.	Instalace .....	16
8.2.2.	Konfigurace .....	17
8.2.3.	Test .....	17
9.	Web .....	18
9.1.	Server XAMPP .....	18
9.1.1.	Instalace .....	18
9.1.2.	Konfigurace .....	18
9.1.3.	Vytvoření jednoduché stránky .....	18
9.1.4.	Firewall .....	18
9.2.	Klient .....	19
9.2.1.	Test .....	19
10.	Závěr .....	20

## 1. Úvod

Úkolem závěrečné práce je zprovoznění řadiče domény společně s politikami a následně přihlásit klientský počítač k této doméně. Dále každý uživatel v doméně bude členem příslušné skupiny a bude se nacházet v příslušné organizační jednotce, dle předem vytvořené struktury. Také je podle zadání práce potřeba nasdílet a namapovat síťové jednotky a nastavit oprávnění přístupu.

Dalším úkolem je instalace emailového serveru Kerio MailServer a následné přihlášení emailového klienta Mozilla Thunderbird k SMTP, IMAP/POP3 účtům. Jeden z bodů zadání říká, že na serveru bude nainstalován FTP server. Neodolal jsem a zvolil OpenSource FTP server FileZilla, který je na rozdíl od CesarFTP stále aktualizovaný a na rozdíl od Cerberus je zcela zdarma. Jeden z posledních úkolů je nainstalovat Apache distribuci XAMPP, která obsahuje komponenty apache2, MySQL, php a další. Pro naše účely podle zadání by stačilo apache, ale neumím si v praxi představit web bez databáze.

V poslední řadě je potřeba nainstalovat roli DHCP serveru a nakonfigurovat jej. Tento krok jsem provedl jako jeden z prvních abych si ušetřil práci.

## 2. Instalace

### 2.1. Windows Server 2019

#### 2.1.1. Vytvoření virtuálního stroje

Vytvoření virtuálního stroje je v hypervisoru VMware Workstation velice jednoduché. V horním panelu v kartě **File** zvolíme volbu **New virtual machine...**

Dále zvolíme typickou konfiguraci (**Typical**). V dalším kroku zvolíme možnost, že nainstalujeme operační systém později (**I will install the operating system later.**), protože pokud vybereme instalační disk již v tomto kroku připojí se později virtuální floppy disk s funkcí Easy Install, což by způsobilo problémy s instalací (možná to v dalších verzích opraví).

V dalším kroku vybereme operační systém **Microsoft Windows**. Bohužel Windows Server verze 2019 není v seznamu systémů, proto vybereme tomu nejbližší **Windows Server 2016**. V dalším kroku pojmenujeme virtuální stroj (toto ale není hostname, ale pouze jméno pod, kterým si VMware Workstation virtuální stroj uloží) a vybereme cestu, kam se budou ukládat soubory virtuálního stroje.

V dalším kroku můžeme kapacitu disku ponechat na výchozí hodnotě, tedy **60GB** a ponechat výchozí nastavení rozdělení virtuálního disku do více souborů (**Split virtual disk into multiple files**).

V dalším kroku klikneme na tlačítko **Customize Hardware...**, kde připojíme síťovou kartu do virtuální sítě a vybereme instalační iso soubor ve virtuální CD/DVD jednotce.

Změny potvrdíme tlačítkem **OK** a dokončíme průvodce tlačítkem **Finish**.

#### 2.1.2. Instalace systému

Po nabootování do instalačního programu vybereme formát času a měny a rozložení klávesnice na **Czech**. V dalším kroku stiskneme tlačítko **Install now**.

Vybereme edici **Windows Server 2019 Standard Evaluation (Desktop Experience)**. Dále si přečteme licenční podmínky a zaškrtneme checkbox **I accept the license terms**.

Dále zvolíme vlastní instalaci (**Custom: Install Windows only (advanced)**) a v dalším kroku vybereme nealokované místo na jednotce (systém si vytvoří oddíly sám).

A nakonec zvolíme heslo administrátora

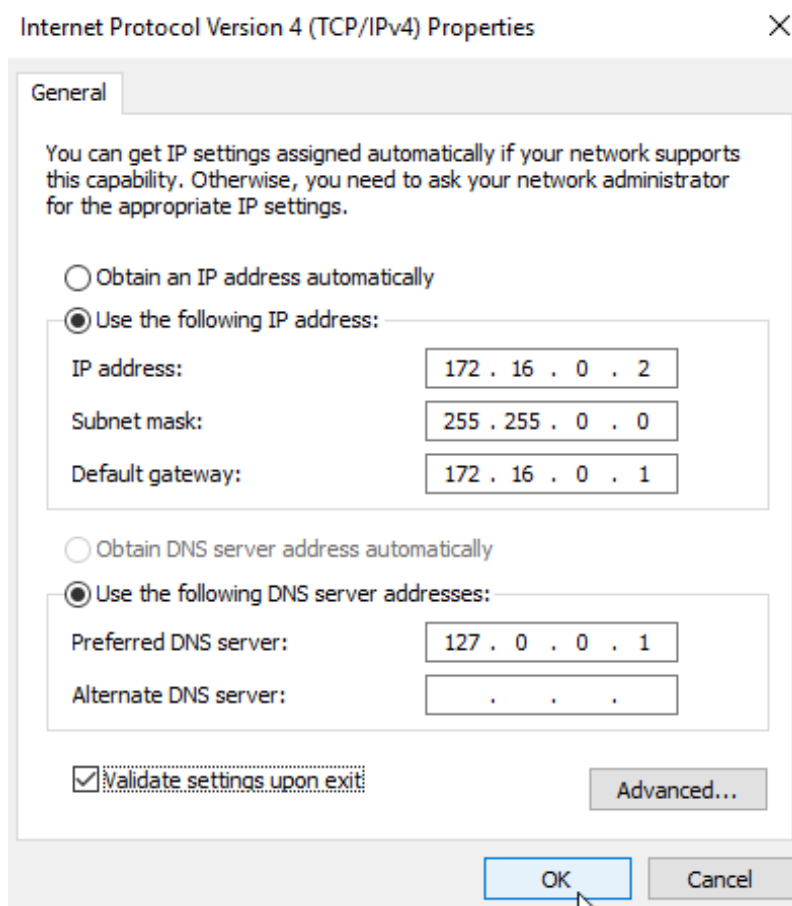
#### 2.1.3. Změna hostname

Otevřeme průzkumníka a pravím kliknutím na **This PC** otevřeme ovládací panely v části **System**, kde v levém panelu klikneme na **Advanced system settings**. V kartě

**Computer Name** klikneme na tlačítko **Change....** Zde změníme jméno počítače na server a virtuální počítač restartujeme.

#### 2.1.4. Konfigurace sítě

Dále je potřeba na síťovém rozhraní nastavit konfiguraci IP. Otevřeme ovládací panely a v políčku cesty napíšeme **Control Panel\Network and Internet\Network and Sharing Center**. Zde v levém panelu klikneme na **Change adapter settings**. Zde se zobrazí rozhraní. Poklepáním na rozhraní se zobrazí okno stavu rozhraní. Zde klikneme na **Properties**. Dále poklikáme na **Internet Protocol Version 4 (TCP/IPv4)**. Zde zadáme konfiguraci IP (důležité je nastavit preferovaný DNS server na loopback 127.0.0.1).



## 2.2. Windows 10

### 2.2.1. Vytvoření virtuálního stroje

Opět v horním panelu v kartě **File** zvolíme volbu **New virtual machine....**

Dále zvolíme typickou konfiguraci (**Typical**). V dalším kroku zvolíme možnost, že nainstalujeme operační systém později (**I will install the operating system later**), protože jsem měl s funkcí Easy Install a novým buildem 1909 problémy.

V dalším kroku vybereme operační systém Microsoft Windows a verzi systému Windows 10 x64. V dalším kroku pojmenujeme virtuální stroj a vybereme cestu, kam se budou ukládat soubory virtuálního stroje.

V dalším kroku můžeme kapacitu disku ponechat na výchozí hodnotě, tedy **60 GB** a ponechat výchozí nastavení rozdělení virtuálního disku do více souborů (**Split virtual disk into multiple files**).

V dalším kroku klikneme na tlačítko **Customize Hardware...**, kde připojíme síťovou kartu do virtuální sítě. Dále vybereme instalační iso soubor ve virtuální CD/DVD jednotce.

Změny potvrdíme tlačítkem OK a dokončíme průvodce tlačítkem **Finish**.

### 2.2.2. Instalace systému

Po nabootování do instalačního programu můžeme ponechat výchozí nastavení a poté klikneme na tlačítko **Nainstalovat**. V dalším kroku klikneme na **Nemám kód Product Key**.

Vybereme edici Windows 10 Pro. Dále si přečteme licenční podmínky a zaškrtneme checkbox **Přijímám licenční podmínky**.

Dále zvolíme vlastní instalaci (**Vlastní: Jenom nainstalovat Windows (pokročilé)**) a v dalším kroku vybereme nealokované místo na jednotce (systém si vytvoří oddíly sám).

Poté co se systém nainstaluje zvolíme oblast a v dalším kroku rozložení klávesnice. Další rozložení klávesnice nepotřebujeme proto klikneme na **Přeskočit**.

Dále musíme počítač odpojit od internetu jinak bude Windows chtít, abychom se přihlásili pomocí účtu Microsoft (pokud jsme ve virtuálním prostředí bez NATu není toto vůbec třeba řešit, také se toto mění sestavení od sestavení). Klikneme na tlačítko **Nemám internet**.

Vyplníme uživatelské jméno třeba **admin** a v následujících dvou krocích napíšeme heslo. Jelikož je tento počítač ve virtuálním prostředí tak jsem zvolil jako odpovědi na bezpečnostní otázky tečku. V praxi bych ale tento účet zrušil a vytvořil nový pomocí **cmd**, protože bezpečnostní otázky jsou značné bezpečnostní riziko.

V následujících krocích zvolíme vše **Ne-** a přijmeme, protože většina funkcí je zbytečných a nechceme Microsoftu odesílat moc dat, takže zvolíme úroveň **Základní**.

Po tomto „buzeračním“ průvodci máme nainstalovaný plně funkční systém.

### 2.2.3. Změna hostname

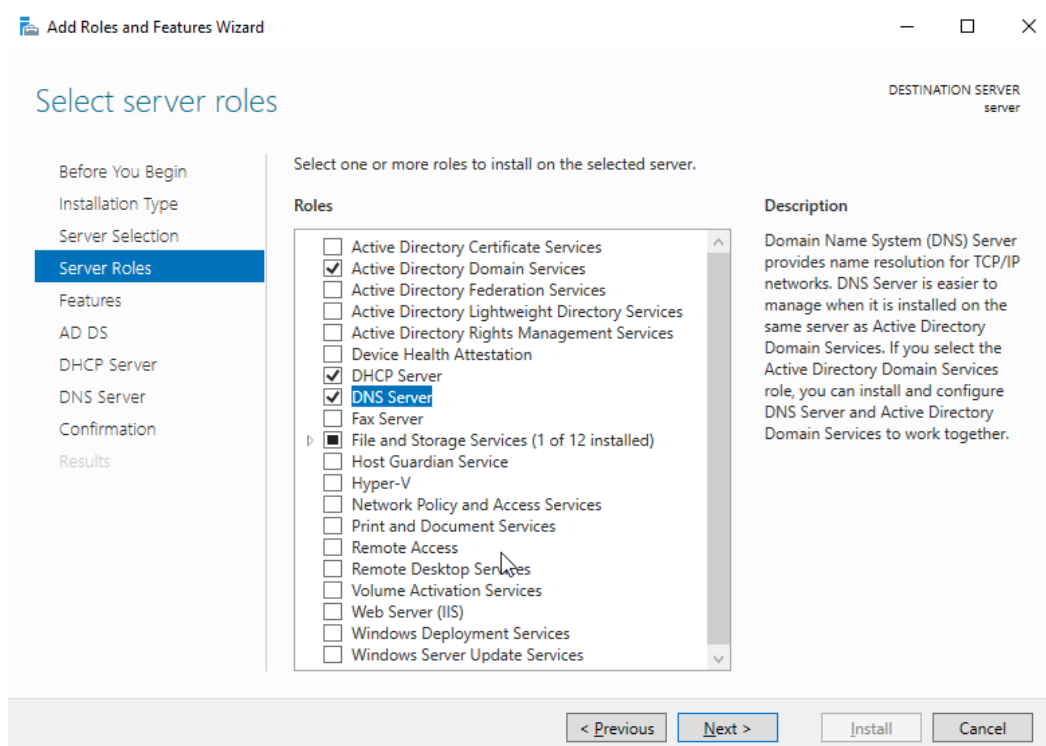
Otevřeme průzkumníka a pravím kliknutím na **Tento počítač** otevřeme ovládací panely v části Systém, kde v levém panelu klikneme na **Upřesnit nastavení systému**. V kartě **Název počítače** klikneme na tlačítko **Změnit....** Zde změníme jméno počítače na server a virtuální počítač restartujeme.

## 3. Instalace a konfigurace rolí

### 3.1. Instalace

Při prvním spuštění se zobrazí okno, které můžeme s klidem v duši ignorovat a aby nás neotravovalo při dalším spuštění zaškrtneme možnost **Don't show this message again**. Pro instalaci rolí klikneme v programu Server Manager na tlačítko **Add roles and features**. Další krok můžeme ignorovat a zaškrtnout možnost **Skip this page by default**, aby se při příštím přidávání rolí a funkcí již nezobrazovala. V dalším kroku zvolíme **Role-based or feature-based installation** a stiskneme **Next**.

V tomto kroku vybereme server a v následujícím kroku zaškrtneme služby, které potřebujeme (**Active Directory Domain Services**, **DHCP Server** a **DNS Server**). Během zaklikávání se budou zobrazovat okna s informací o instalovaných komponentách, které pokaždé potvrdíme stisknutím **Add Features**.



Další čtyři okna proklikáme, protože obsahují jen informace o instalovaných rolích. V dalším okně máme přehled všech instalovaných rolí a funkcí, které potvrdíme tlačítkem **Install**. Mým zvykem je, pokud není potřeba, aby server běžel, tak zaškrtnout možnost **Restart the destination server automatically if required**, která automaticky restartuje server, pokud to bude potřeba (v tomto případě to potřeba není). Po dokončení instalace můžeme okno zavřít.

### 3.2. DHCP Server

#### 3.2.1. Server

V Server Manager klikneme na **ikonu úloh** (šedá vlaječka) a klikneme na **Complete DHCP configuration**. Nově zobrazené okno stačí proklikat.



Kliknutím na DHCP v levém panelu se zobrazí seznam serverů a událostí, kde pravým tlačítkem klikneme na server a v kontextové nabídce vybereme **DHCP Manager** nebo přes tlačítko **Tools** zvolíme **DHCP**.

V konfiguraci DHCP rozbalíme strukturu po IPv4. Na tuto položku klikneme pravým tlačítkem a zvolíme **New Scope**, tím spustíme průvodce novým oborem DHCP. V prvním kroku zadáme jméno a popis.

Dále zvolíme adresní prostor, se kterým bude DHCP server pracovat a dole zvolíme CIDR a masku podsítě. V dalším kroku vyloučíme IP adresy, které nechceme, aby DHCP server dynamicky přiřazoval. Tedy já jsem vyloučil jednu IP adresu pro výchozí bránu (router), pro tento server a adresní prostor pro případné zařízení, u kterých je potřeba, aby se jejich IP adresa neměnila (např. tiskárny, ...).

The image displays two side-by-side screenshots of the 'New Scope Wizard' in Windows Server.

**Left Screenshot: IP Address Range**  
The title is 'IP Address Range'. The subtitle says: 'You define the scope address range by identifying a set of consecutive IP addresses.'  
Under 'Configuration settings for DHCP Server', it says: 'Enter the range of addresses that the scope distributes.'  
Start IP address: 172 . 16 . 0 . 1  
End IP address: 172 . 16 . 255 . 254  
Under 'Configuration settings that propagate to DHCP Client', it says:  
Length: 16  
Subnet mask: 255 . 255 . 0 . 0  
At the bottom are buttons: '< Back', 'Next >', and 'Cancel'.

**Right Screenshot: Add Exclusions and Delay**  
The title is 'Add Exclusions and Delay'. The subtitle says: 'Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.'  
It says: 'Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.'  
Start IP address: [ ] End IP address: [ ] Add  
Excluded address range:  
Address 172.16.0.1  
Address 172.16.0.2  
172.16.0.3 to 172.16.0.20  
Remove  
Subnet delay in milli second: 0  
At the bottom are buttons: '< Back', 'Next >', and 'Cancel'.

V tomto kroku zvolíme lease time neboli dobu propůjčení IP adresy (tuto hodnotu volíme podle toho kolik máme IP adres v adresním prostoru a po jakou průměrnou dobu se budou zařízení nacházet v síti, aby se mohli uvolnit a nečerpal se tak zbytečně adresní prostor). V kroku dalším zvolíme **Yes, I want to configure these options now**, abychom nakonfigurovali další potřebné nastavení.

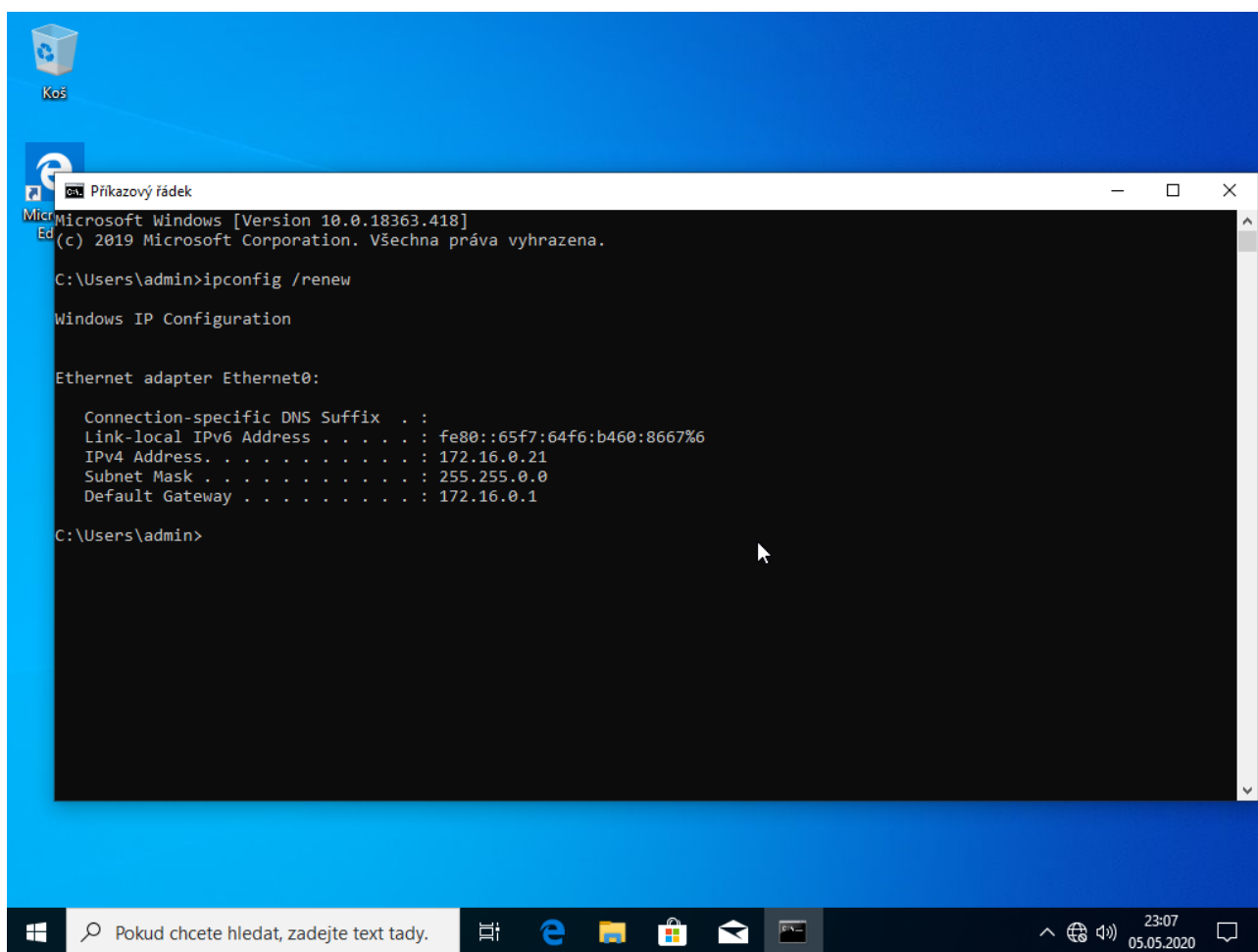
V tomto kroku zvolíme výchozí bránu. V následujícím kroku vybereme DNS server, kterým je tento server.

Okno s konfigurací WINS můžeme přeskočit a v dalším kroku zvolíme **Yes, I want to activate this scope now**, což aktivuje námi nově vytvořený obor.

Průvodce ukončíme stisknutím tlačítka **Finish**.

### 3.2.2. Klient

V tuto chvíli můžeme restartovat klientský počítač nebo spustit v cmd příkaz **ipconfig /renew**, který provede DHCP release a odešle požadavek DHCP discover a tak dále. Jednoduše řečeno získá IP adresu od DHCP serveru.



### 3.3. Řadič domény

#### 3.3.1. Server

V Server Manager klikneme opět na **ikonu úloh** (šedá vlaječka). Dále klikneme na **Promote this server to a domain controller**. V novém okně zvolíme **Add a new forest** a zadáme požadované jméno domény (**nemocnice.local**).

Dále zvolíme **Forest functional level: Windows Server 2016**, protože nepotřebujeme zpětnou kompatibilitu se staršími systémy Windows Server. Další kartu přeskočíme.

V dalším kroku se automaticky vygeneruje doména pro NetBIOS, zde a v dalším kroku, kde se nastavují cesty k databázím, stačí kliknout další, protože tyto hodnoty nepotřebujeme měnit. Dále se nám zobrazí přehled, který také jen proklikneme a v dalším kroku stačí zmáčknout tlačítko **Install**. Server se po instalaci restartuje.

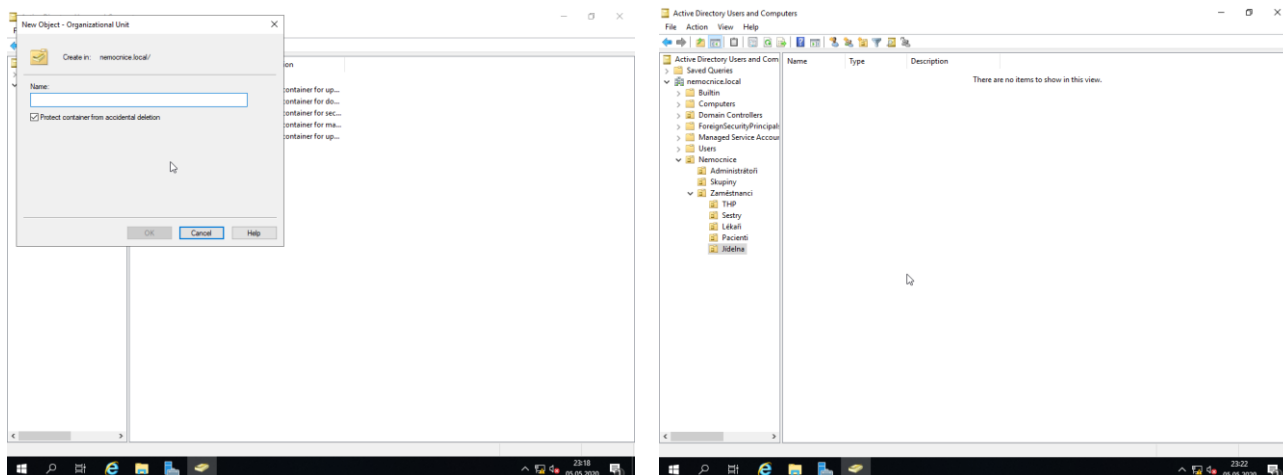
#### 3.3.2. Klient

Nyní už můžeme klientský počítač připojit do domény pomocí účtu **Administrator**, a to na stejném místě, jako jsme měnili hostname viz. Změna hostname. A poté restartujeme počítač.

## 4. Konfigurace Active Directory

### 4.1. Organizační jednotky

Nástroj **Active Directory Users and Computers** spustíme kliknutím na **Tools** a následně vybereme **Active Directory Users and Computers**. Ve struktuře kliknutím pravým tlačítkem na doménu (nemocnice.local) otevřeme kontextovou nabídku a tam najedeme na **New** a zvolíme **Organizational Unit**. Do nového okna napíšeme název organizační jednotky (**Nemocnice**). Já osobně neodškrtnávám volbu **Protect container from accidental deletion**, protože není až tak těžké tento nastavení z organizační jednotky odstranit. Dále stejným způsobem vytvoříme následující strukturu:



### 4.2. Domovský adresář

Dále vytvoříme v kořenovém adresáři složku **Home**, která bude sloužit pro domovské složky uživatelů. Složku nasdílíme tak, že na ni klikneme pravým tlačítkem a zvolíme **Properties**. Zde v kartě **Sharing** klikneme na **Advanced Sharing...** Zde zaškrtneme **Share this folder** a do **Share name** napíšeme název sdílené složky (**Home**). Dále nastavíme oprávnění, a to kliknutím na **Permissions**, kde u **Everyone** zaškrtneme ve sloupečku **Allow** možnosti **Read** a **Change** a vše potvrdíme tlačítkem **OK**. Následně ve složce **Home** vytvoříme strukturu podobnou té v **Active Directory** z organizačních jednotek s tím rozdílem, že není potřeba vytvářet složku pro **Skupiny**. Pro tento účel by se dal vytvořit logon skript.

### 4.3. Skupiny

Dále v **Active Directory Users and Computers** v organizační jednotce **Skupiny** vytvoříme skupinu pro každou organizační jednotku. Vytvoříme ji tak, že klikneme pravým tlačítkem na organizační jednotku **Skupiny**, poté najedeme na **New** a poté klikneme na **Group**. Zde vyplníme název skupiny. Spodního pole si nemusíme všimnout, protože nepoužíváme žádné speciální znaky. **Group scope** a **Group type** ponecháme na výchozích hodnotách (**Global**, **Security**).

Dále skupině Administrátoři přidáme členství v systémových skupinách a to **Domain Users, Domain Admins, Administrators, Remote Desktop Users**) a to tak, že kliknutím pravým tlačítkem otevřeme kontextovou nabídku a v ní vybereme **Properties**. Zde v kartě **Member Of** klikneme na tlačítko **Add...**, které otevře nové okno. V tomto okně se nachází textové pole, do kterého vepíšeme název skupiny a zkontrolujeme název tlačítkem **Check Names** pokud se skupina podtrhne je napsaná správně, následně zmáčkeme tlačítko **OK**.

#### 4.4. Uživatelé

Dále pro každou organizační jednotku vytvoříme uživatele tak, že klikneme pravým tlačítkem na danou organizační jednotku, poté najedeme na **New** a poté klikneme na **User**. Vyplníme jméno, příjmení a případně iniciály. Celé jméno se generuje automaticky. Zvolíme **User logon name** (nejlépe jen malá písmena bez diakritiky). Na další stránku pokračujeme tlačítkem **Next**. Zde dvakrát napíšeme výchozí heslo uživatele, který si uživatel po přihlášení změní (pokud ponecháme zaškrtlé **User must change password at next login**). Pokračujeme tlačítkem **next**. V další části průvodce máme přehled nastavení. Tento průvodce dokončíme stisknutím **Finish**.

Dále přidáme uživatele do skupiny, to uděláme tak, že klikneme pravým tlačítkem myši na uživatele a vybereme **Properties**. Dále přepneme na kartu **Member Of** a klikneme na tlačítko **Add**. Zde napíšeme jméno skupiny a zmáčkeme tlačítko **Check Names**. Pokud se skupina podtrhne napsali jsme název správně, poté můžeme potvrdit tlačítkem **OK**.

Když už máme otevřené okno **Properties**, můžeme přepnout na kartu **Profile**. Zde v části **Home Folder** zaklikneme **Connect** vybereme písmeno jednotky **X:** a do vedlejšího textového pole vepíšeme síťovou cestu **\\server.nemocnice.local\Home\Složka dle organizačních jednotek\%username%** (místo FQDN lze použít jen hostname nebo IP adresu, wildcart **%username%** doplní uživatelské jméno) a vše potvrdíme tlačítkem **OK**. Dále je potřeba zakázat dědění nově vytvořené domácí složky někde v adresáři **C:\Home**. Po nalezení složky se jménem uživatele na ni klikneme pravým tlačítkem a zvolíme **Properties**. Zde se přepneme na kartu **Security**, kde zmáčkeme tlačítko **Advanced**. V nově otevřeném okně stiskneme tlačítko **Disable inheritance**. Tímto zakážeme dědění oprávnění od nadřazených adresářů. Vytvoří se ještě jedno okno, ve kterém odklikneme **Remove all inherited permissions from this object**.

Tyto dva kroky provedeme u všech uživatelů.

## 5. Vytvoření a mapování jednotek

### 5.1. Sdílení adresářů

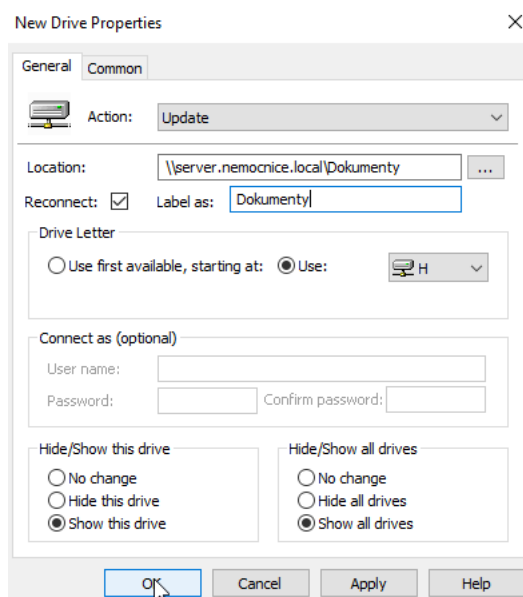
V kořenovém adresáři vytvoříme novou složku **Nemocnice** a v ní tři další – **Dokumenty**, **Instalace** a **Lékařské zprávy**. Každou z těchto složek nasdílíme a to tak, že klikneme pravým tlačítkem na složku a zvolíme **Properties**. Zde v kartě **Sharing** zmáčkneme tlačítko **Advanced Sharing...** Zde opět zaškrtneme **Share this folder** a do **Share name** napíšeme název sdílené složky. Dále nastavíme oprávnění, a to kliknutím na **Permissions**, kde u **Everyone** zaškrtneme ve sloupečku **Allow** možnosti **Read** a **Change** a vše potvrdíme tlačítkem **OK**.

Dále v kartě **Security** klikneme na tlačítko **Edit...** a přidáme všechny skupiny z organizační jednotky **Skupiny** a povolíme jim či zakážeme různé oprávnění. **Administrátoři** budou mít plnou kontrolu. Skupinu přidáme tak že v tomto okně zmáčkneme tlačítko **Add...** a zde napíšeme název skupiny. Poté zmáčkneme tlačítko **Check Names** a pokud se jméno skupiny podtrhne, tak jsme jej zadali správně a potvrdíme formulář tlačítkem **OK**. Poté vybereme skupinu v seznamu v horní části okna a v dolní části nastavíme oprávnění.

### 5.2. Vytvoření objektu skupinové politiky (GPO)

V **Run** nebo přes vyhledávací pole spustíme **mmc** a otevře se nám program **Group Policy Management**. Zde v levém panelu rozbalíme strukturu po organizační jednotku **Nemocnice**, na kterou klikneme pravým tlačítkem a vybereme možnost **Create a GPO in this domain, and Link It here....** Dále do pole **Name:** napíšeme název objektu (**mapovani**) a potvrdíme tlačítkem **OK**.

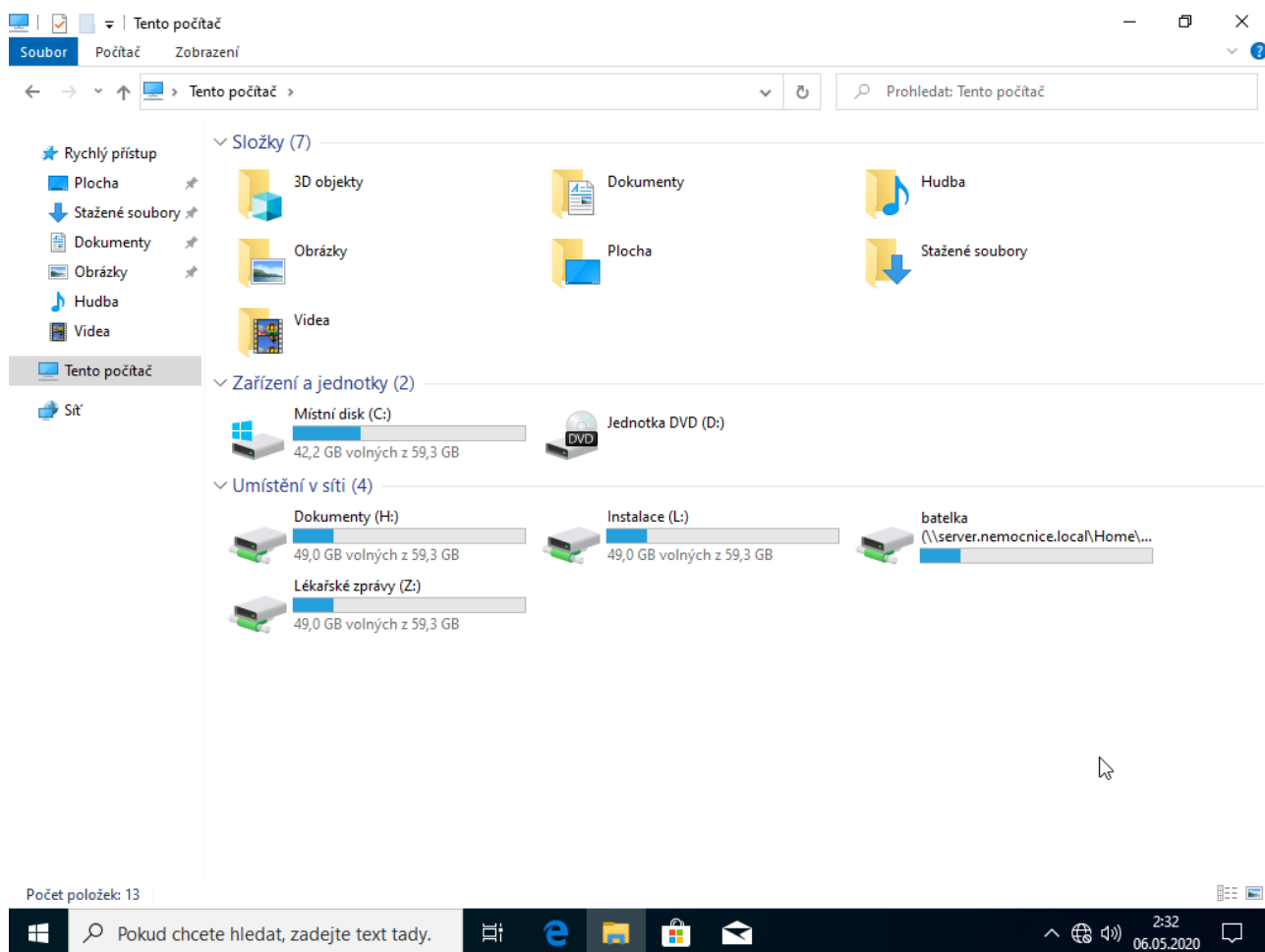
Poté klikneme pravým tlačítkem na vytvořený objekt a vybereme **Edit...** Zde ve strukturovaném seznamu rozbalíme **User Configuration – Preferences – Windows Settings** a rozklikneme **Drive Maps**.



Nyní v horní části okna klikneme na **Add a new item** (symbol +) a tím se otevře nové okno. Kde **Action:** vybereme **Update**, jako **Location** nastavíme \\ + IP/hostname/FQDN serveru + cesta k adresáři (např. \\server.nemocnice.local\Dokumenty). Dále zaškrtneme možnost **Reconnect:** a do pole **Label as:** napíšeme požadované jméno jednotky (**Dokumenty**). Dále v části **Drive Letter** vybereme **Use** a v rozbalovací nabídce vybereme písmeno jednotky (**H:**). A nakonec v dolní části vybereme **Show this drive** a hned vedle **Show all drives**. Vše nakonec potvrdíme tlačítkem **OK**.

### 5.3. Test

Po odhlášení a přihlášení uživatele nebo po provedení příkazu **gpupdate /force** můžeme vidět, že všechny jednotky máme namapované správně.



## 6. Nastavení politik

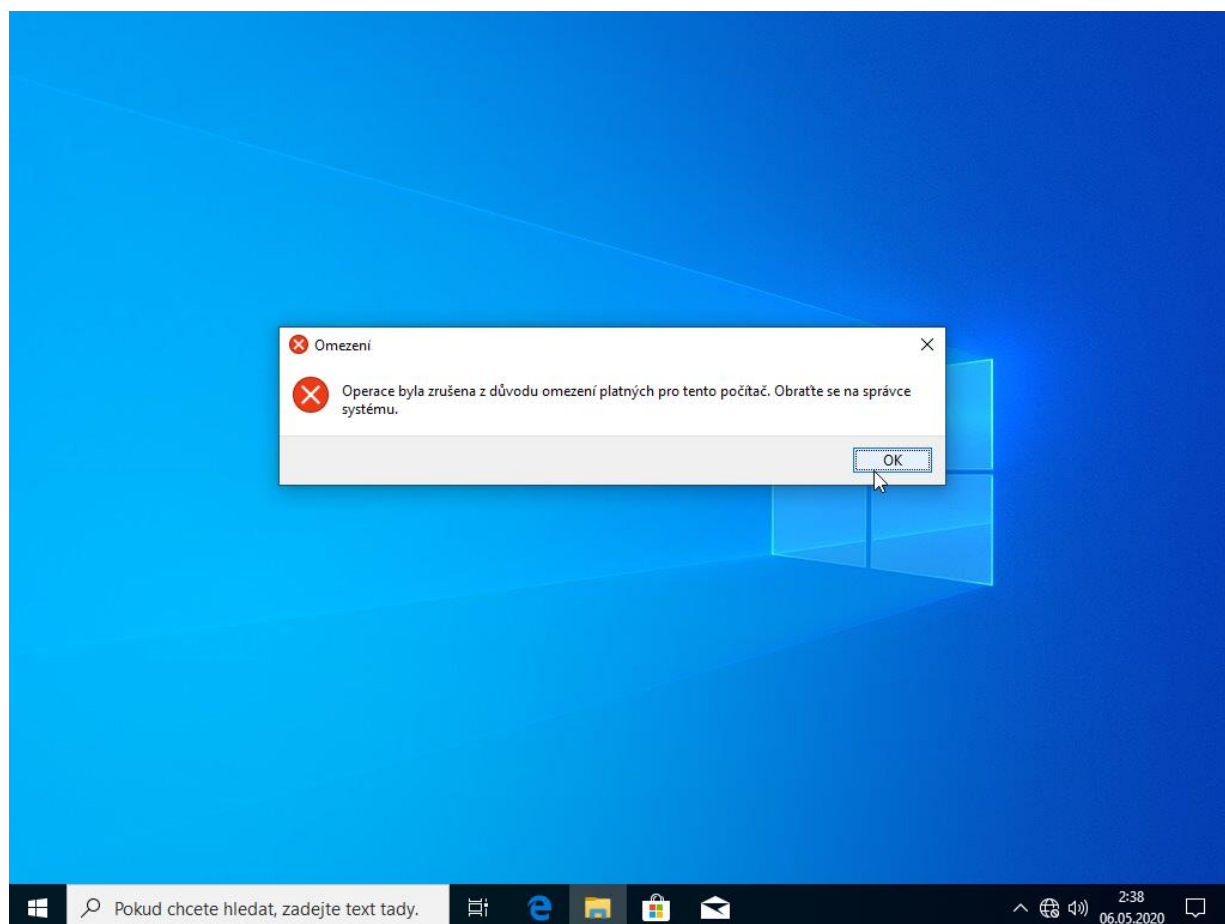
### 6.1. Konfigurace

V **Run** nebo přes vyhledávací pole spustíme **mmc** a otevře se nám program **Group Policy Management**. Zde v levém panelu rozbalíme strukturu po organizační jednotku **Zaměstnanci**, na kterou klikneme pravým tlačítkem a vybereme možnost **Create a GPO in this domain, and Link It here....** Dále do pole **Name:** napíšeme název objektu (**politiky**) a potvrdíme tlačítkem **OK**.

Poté klikneme pravým tlačítkem na vytvořený objekt a vybereme **Edit....** Zde ve strukturovaném seznamu rozbalíme **User Configuration – Policies – Administrative templates – Desktop** a rozklikneme nastavení **Hide and disable all items on the desktop**. V novém okně vybereme **Enabled** a potvrdíme tlačítkem **OK**. V tuto chvíli jsme skryli ikony na ploše. Dále rozklikneme také v **Administrative Templates – Control Panel**. Zde rozklikneme **Prohibit access to Control Panel and PC settings**, abychom zakázali přístup do nastavení a ovládacích panelů. V novém okně opět vybereme **Enabled** a potvrdíme tlačítkem **OK**.

### 6.2. Test

Na níže uvedeném snímku obrazovky můžeme vidět, že na ploše jsou skryté všechny ikony a při pokusu o otevření ovládacích panelů se zobrazí okno informující o omezení nově vytvořenou politikou.





## 7. Mail

### 7.1. Kerio MailServer

#### 7.1.1. Instalace

Poté co spustíme instalační soubor, se zobrazí okno, ve kterém zvolíme jazyk instalace. Já preferuji jazyk anglický proto jsem vybral volbu **Anglicky** a potvrdil tlačítkem **OK**.

V následujících dvou krocích stačí kliknout **Next**, zde totiž není potřeba nic jiného dělat. Ve třetím kroku je potřeba přijmout licenční podmínky volbou **I accept the terms in the license agreement** a následně můžeme pokračovat na další část instalace. Dále máme možnost vybrat instalované komponenty, my ale tuto možnost nepotřebujeme a tedy nainstalujeme kompletní program – vybereme **Complete** a stiskem **Next** pokračujeme dále. V dalším kroku můžeme ponechat výchozí cestu. Dále vybereme jméno administrátora (můžeme ponechat **Admin**) a zvolíme pro uživatele heslo. Dále přichází nejdůležitější bod a to je správné zvolení domény – **nemocnice.local**. V dalším kroku vyplníme FQDN serveru (tedy **server.nemocnice.local**). Nastavení z dalšího kroku opět nepotřebujeme a stačí jej prokliknout. V dalším kroku už můžeme tlačítkem **Install** program nainstalovat. Nyní už stačí instalaci dokončit tlačítkem **Finish**.

#### 7.1.2. Konfigurace

Po spuštění programu **Administration Console** vyplníme údaje pro připojení k serveru (**Produkt: Kerio MailServer, Server: localhost/IP/FQDN, Username: Admin** a heslo uživatele) a klikneme na tlačítko **Save As...**, tím si vytvoříme připojení a nebudeme ho muset znovu konfigurovat. V novém okně zvolíme jméno (postačí výchozí – **localhost**) a uložíme tlačítkem **Save**. Po připojení se zobrazí nové okno **Welcome**, kde můžeme zaškrtnout možnost **In the future, do not show this message**, aby se toto okno už nezobrazovalo a zavřeme jej tlačítkem **Close**.

Nyní si v levém panelu rozklikneme **Services** a upravíme porty, které budeme později potřebovat pro webový server. Proto vybereme službu **HTTP** a zmáčkneme tlačítko **Edit...**. Zobrazí se nové okno, ve kterém znovu stiskneme **Edit...** a zobrazí se další okno, ve kterém upravíme číslo portu (třeba na **8080**) a všechna okna „odklikáme“ tlačítkem **OK**.

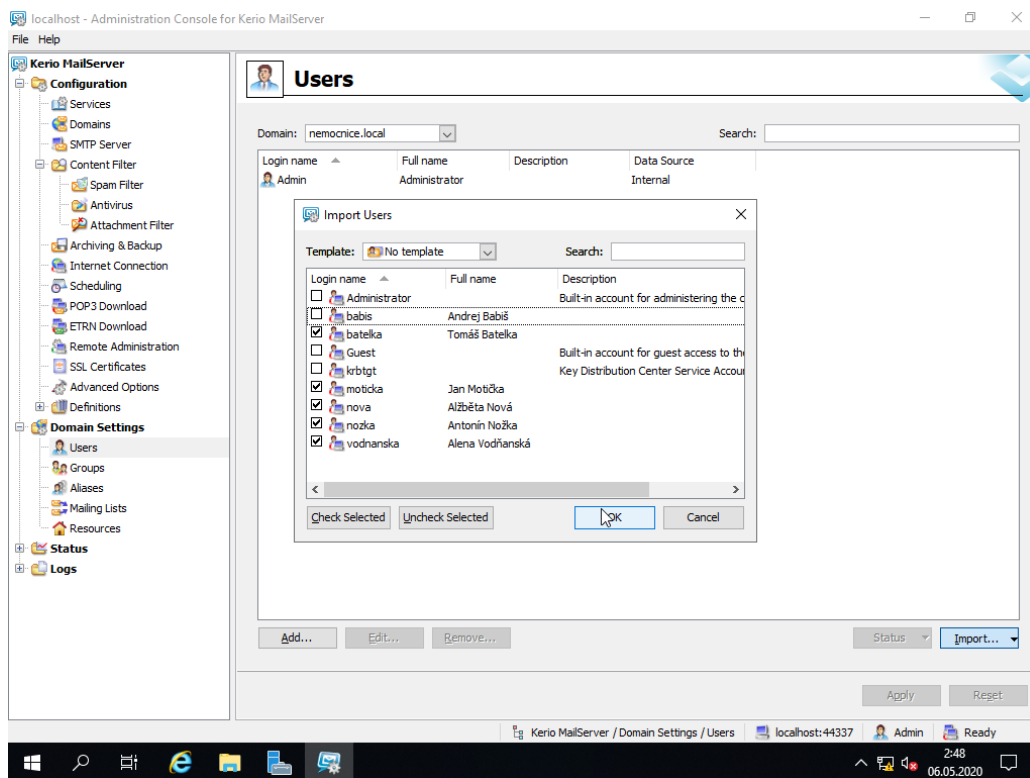
Totéž provedeme i u **HTTPS – Secure HTTP**, kde ale port změníme třeba na **8443**. Poté aplikujeme změny tlačítkem **Apply**. V dalším novém okně stiskneme **Restart**, pro restartování těchto služeb.

Dále v **Configuration – SMTP Server** vybereme **Open relay** (v praxi nepoužívat). Dále v kartě **Queue Options** nastavíme **Send the sender a warning if the message is not delivered after:** na **1 minutes**, tedy uživatel dostane informaci o nedoručeném emailu už po jedné minutě, všechny změny poté aplikujeme.

V **Configuration – Content Filter – Antivirus** odškrtneme možnost **Use integrated McAfee® antivirus engine**, protože tento antivirus často působí problémy a aplikujeme změny.



Dále v **Domain Settings – Users** importujeme uživatele z AD tlačítkem **Import...** (tím si usnadníme trochu práci). V nabídce vybereme **Import from directory service...**. V nabídce **Import users from** vybereme **Windows NT® Domain (Windows NT® 4.0)**. Jako doménové jméno zvolíme **nemocnice.local**, možnost **LDAPS** není potřeba vzhledem k tomu že se mail-server nachází na stejném stroji jako řadič domény. Po stisknutí tlačítka **OK** se zobrazí nové okno se seznamem uživatelů, kde vybereme všechny uživatele krom těch systémových a pacientů.



Dále poklepáním na uživatele každého importovaného uživatele upravíme a to tak, že u **Authentication** vybereme **Internal user database** a pod tuto nabídku napíšeme dvakrát heslo. Vše potvrdíme tlačítkem **OK**.

Dále pro všechny uživatele nastavíme POP3 účet. To provedeme v **Configuration – POP3 Download**, kde stiskneme tlačítko **Add...** pro přidání účtu. Dále vyplníme **POP3 server: localhost**, **POP3 username** a **password**. Dále nesmíme zapomenout vybrat tlačítkem **Select...** emailovou schránku, do které budou emaily doručovány. Zde vybereme uživatele v seznamu a potvrdíme.

### 7.1.3. Firewall

Také je potřeba povolit port ve Windows Defender Firewall, který můžeme spustit přes pole hledání **wf.msc**, kde zvolíme položku **Inbound Rules**. Povolit port můžeme dvojím způsobem. Buď v prvním okně vybereme **Program**, dále vybereme cestu k programu **%ProgramFiles% (x86)\Kerio\MailServer\mailserver.exe**, dále vybereme **Allow the connection**, v dalším kroku můžeme ponechat zaškrtnuté všechny tři profily, dále zvolíme jméno pravidla (**Kerio MailServer**) a popis. Nebo můžeme podobným způsobem povolit porty 25, 465, 110, 995, 143, 993, 8080 a 8443 (119, 563 - NNTP není potřeba povolovat).

## 7.2. Mozilla Thunderbird klient

### 7.2.1. Instalace

Po spuštění instalačního souboru se zobrazí UAC formulář, ve kterém klikneme na **Ano**. V prvním kroku stačí kliknout **Další**. V tom druhém můžeme ponechat **Standartní** instalaci a můžeme ponechat zaškrtnou možnost **Použít aplikaci Thunderbird jako výchozího poštovního klienta**. V kroku dalším už aplikaci nainstalujeme tlačítkem **Instalovat**. A nakonec můžeme ponechat zaškrtnuté tlačítko **Spustit Mozilla Thunderbird** a zmáčknout tlačítko **Dokončit**.

### 7.2.2. Konfigurace

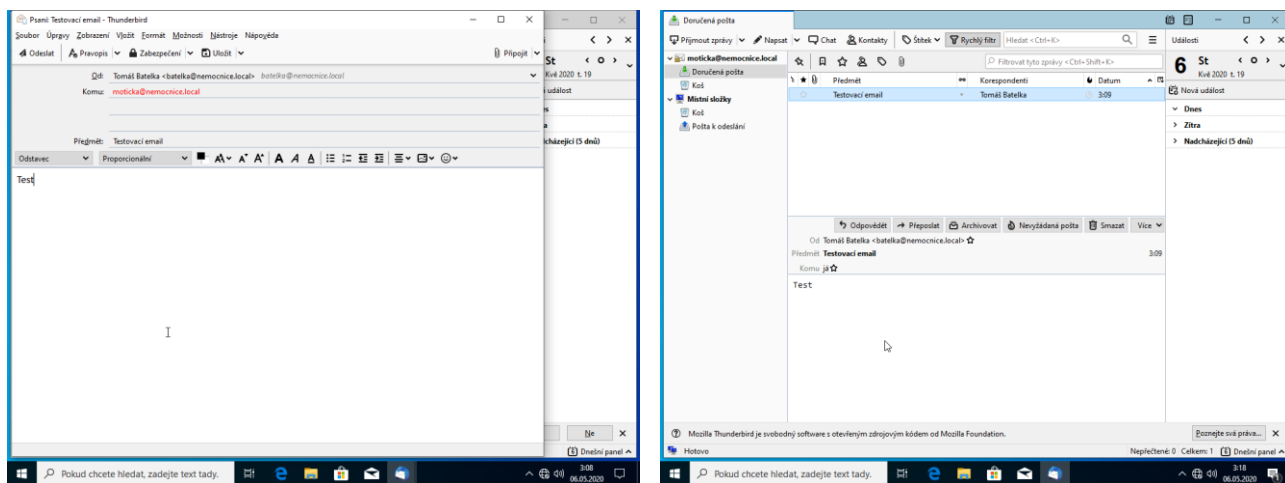
Po spuštění klienta se zobrazí i druhé konfigurační okno, které zavřeme, protože je v této verzi programu chyba. Poté stiskneme na klávesnici levý **Alt**, tím se zobrazí nahoře nabídka. Kurzorem najedeme na **Nástroje** a zde klikneme na **Nastavení účtu**. Poté vlevo dole rozklikneme **Akce účtu** a vybereme **Přidat poštovní účet...**. Pote se zobrazí okno, ve kterém můžeme **Vaše jméno** ponechat a vyplníme tedy emailovou adresu a heslo (možnost **Pamatovat si heslo** můžeme ponechat zaškrtnutou). Nyní můžeme zmáčknout **Pokračovat**. Dále vybereme možnost **IMAP** a zmáčkneme **Hotovo**.

Dále protože nemáme na serveru vygenerovaný certifikát musíme schválit všechny bezpečnostní výjimky tlačítkem **Schválit tuto bezpečnostní výjimku** (možnost **Uložit tuto výjimku trvale** můžeme ponechat zaškrtnou).

Konfigurace **POP3** je obdobná akorát v bodě, kdy vybíráme protokol pro příchozí poštu zvolíme možnost **POP3**.

### 7.2.3. Test

Nyní už můžeme email otestovat. Na níže umístěných snímcích obrazovky je vidět, že email byl z jednoho emailového účtu opravdu doručen na druhý.



## 8. FTP

### 8.1. FTP server

#### 8.1.1. Instalace

Po spuštění exe souboru a potvrzení UAC formuláře přijmeme licenční podmínky tlačítkem **I Agree**. V dalším kroku ponecháme typ instalace **Standard**. V následujícím kroku ponecháme výchozí umístění instalace. Dále můžeme vybrat jak bude FileZilla Server spouštěn a port administrátorského rozhraní, obě nastavení můžeme ponechat na výchozí hodnotě (**Install as service, started with Windows(default), 14147**). V dalším kroku vybereme možnost spuštění administračního rozhraní na manuální (**Start manually**) a možnost **Start Interface after setup completes** můžeme ponechat **zaškrtnout**. Dále už tlačítkem **Install** provedeme samotnou instalaci. Instalační program zavřeme tlačítkem **Close**.

#### 8.1.2. Konfigurace

Nyní tlačítkem **Groups** (ikona dvou hlav a počítače v pozadí) otevřeme okno, kde přidáme novou skupinu a to tak, že klikneme na tlačítko **Add**. Do nově otevřeného okna napíšeme název skupiny (**Administrátoři**). Dále překlikneme na stránku **Shared folders**, kde tlačítkem **Add** přidáme adresář (**C:\Nemocnice**). Dále vybereme tento adresář v nabídce a klikneme na tlačítko **Set as home dir** a v pravém panelu nastavíme všechna oprávnění.

Dále tlačítkem **users**, které symbolizuje ikona jedné hlavy a počítače, otevřeme okno **Users**, ve kterém můžeme přidat uživatele. Uživatele přidáme stisknutím tlačítka **Add**. V novém okně zvolíme uživatelské jméno a příslušnou skupinu (**Administrátoři**). Dále tento účet vybereme v nabídce **Users** a zaškrtneme **Enable account** a **Password**, kde ve vedlejším poli vepíšeme heslo a vše potvrdíme tlačítkem **OK**.

#### 8.1.3. Firewall

Dále je potřeba povolit port ve Windows Defender Firewall, který můžeme spustit přes pole hledání **wf.msc**, kde zvolíme položku **Inbound Rules**. Povolit port můžeme dvojím způsobem. Buď v prvním okně vybereme **Program**, dále vybereme cestu k programu **%ProgramFiles%\FileZilla Server\ FileZilla Server.exe**, dále vybereme **Allow the connection**, v dalším kroku můžeme ponechat zaškrtnuté všechny tři profily, dále zvolíme jméno pravidla a popis. Nebo můžeme podobným způsobem povolit port 21 a pro administraci port 14147.

### 8.2. FTP klient

#### 8.2.1. Instalace

Po spuštění instalačního souboru se zobrazí UAC (User Access Control) formulář, který potvrdíme stisknutím tlačítka **Ano**. Dále přijmeme licenční podmínky tlačítkem **I Agree**. Na další stránce vybereme, pro jaké uživatele FTP klienta nainstalujeme. Dále vybereme komponenty, které chceme nainstalovat (já jsem si navíc zaškrtnl **Desktop Icon**). V dalším kroku vybereme umístění instalace a dále máme možnost vybrat, do jaké složky v menu se vytvoří zástupce FTP klienta. Po tomto kroku se provede

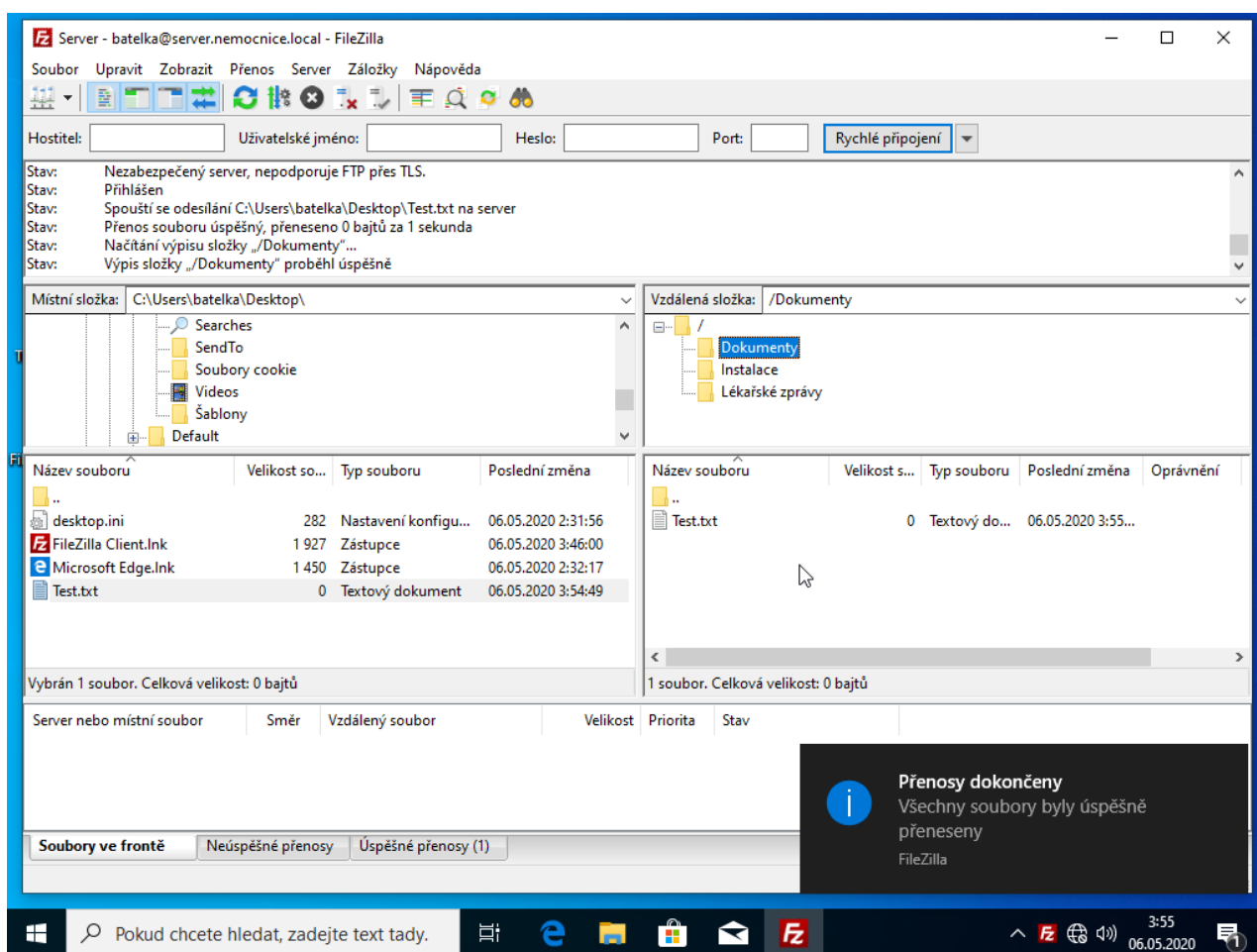
samotná instalace. Po dokončení instalace máme možnost spustit klienta ihned po stisknutí tlačítka Finish, kterou ponecháme zaškrtnou.

### 8.2.2. Konfigurace

Po spuštění programu FileZilla zmáčkneme tlačítko **Správce míst** (ikona tří serverů). Tím se otevře nové okno, kde stiskneme tlačítko **New site**. V pravé části okna vyplníme informace o serveru a způsob autentifikace. Tedy vybereme **Protokol: FTP - File Transfer Protokol**, **Hostitel: server.nemocnice.local** nebo **IP adresu serveru**, port využíváme výchozí (21), takže nemusíme vyplňovat, šifrování můžeme ponechat na výchozí hodnotě, i když TLS nemáme na serveru nakonfigurovaný. **Způsob přihlašování** zvolíme **Normální**, zadáme uživatelské jméno a heslo. Nyní už se můžeme k serveru připojit. V novém okně můžeme nechat zaškrtnuté **Ukládat hesla**. V dalším okně můžeme zaškrtnout **Always allow insecure plain FTP for this server**, aby se už toto okno nezobrazovalo. Nyní už jsme úspěšně připojeni k FTP serveru a nacházíme se v kořenovém adresáři, který jsme nakonfigurovali na serveru.

### 8.2.3. Test

Nyní můžeme zkusit přenos souboru. Na smímku obrazovky můžeme vidět, že se soubor opravdu přenesl.



## 9. Web

### 9.1. Server XAMPP

#### 9.1.1. Instalace

První krok po spuštění instalačního souboru můžeme přeskočit. V dalším kroku můžeme vybrat, které komponenty chceme nainstalovat, pro splnění zadání stačí ponechat pouze Apache, ale neumím si představit server bez databáze a nějakého back-endu (takže jsem zaškrtnul i **MySQL**, **PHP**, **Perl** a **phpMyAdmin**). V dalším okně vybereme cestu pro instalaci. Můžeme ponechat výchozí hodnotu. Já ale mám radši, když se programy instalují tam kam ostatní, proto jsem změnil cestu na: **C:\Program Files\xampp**. Jazyk ponecháme **English** a další dvě ona proklikneme tlačítkem **Next >**. Tím máme instalaci hotovou a dokončíme ji tlačítkem **Finish**.

#### 9.1.2. Konfigurace

Po spuštění programu **XAMPP Control Panel**. Nainstalujeme moduly jako služby. To uděláme kliknutím na křížek u jednotlivého modulu a potvrzením stisknutím **Yes** v novém okně (toto uděláme u obou modulů **Apache** i **MySQL**). Nyní už obě služby můžeme spustit stisknutím tlačítka **Start**.

#### 9.1.3. Vytvoření jednoduché stránky

V dalším kroku otevřeme libovolný textový editor a vytvoříme jednoduchou HTML stránku. Postačí k tomu i aplikace **Notepad**.

```
<!DOCTYPE html>
<html>
  <head>
    <title>Intranet</title>
  </head>
  <body>
    <h1>Intranet</h1>
  </body>
</html>
```

Zvolíme **File** dále **Save As**. V novém okně vybereme cestu tedy **C:\xampp\htdocs** v mém případě **C:\Program Files\xampp\htdocs**. Vybereme **Encoding: UTF-8**, kvůli správnému zobrazení českých znaků a jméno souboru bude **index.html**.

#### 9.1.4. Firewall

Také je potřeba povolit port ve Windows Defender Firewall, který můžeme spustit přes pole hledání **wf.msc**, kde zvolíme položku **Inbound Rules**. Povolit port můžeme dvojím způsobem. Buď v prvním okně vybereme **Program**, dále vybereme cestu k programu **%ProgramFiles%\xampp\apache\bin\httpd.exe**, dále vybereme **Allow the connection**, v dalším kroku můžeme ponechat zaškrtnuté všechny tři profily, dále zvolíme jméno pravidla a popis. Nebo můžeme podobným způsobem povolit port 80 a 443. Port 3306 nemusíme povolovat vzhledem k tomu, že se webový server nachází na místním serveru a tedy není potřeba vzdálené připojení.

## 9.2. Klient

### 9.2.1. Test

Po zadání URL adresy FQDN serveru **server.nemocnice.local** se zobrazí nápis **Intranet**, tímto způsobem zjistíme, že webový server opravdu funguje.



## Intranet



## 10. Závěr

Nakonec si myslím, že práce dopadla úspěšně. Všechny role na serveru se podařilo zprovoznit a všechny služby se spouští automaticky po startu serveru. Při plnění zadání jsem nenarazil na žádný problém (tedy až na tu chybu, kterou má Mozilla Thunderbird).