Univerzita Hradec Králové
Fakulta informatiky a managementu
KIT – Katedra informačních technologií

Hardening operačních systémů

Bakalářská práce

Autor: Vladislav Ivančo
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Tomáš Svoboda, Ph.D.

Hradec Králové 19.04.2024

Prohlášení:

Prohlašuji, že jsem bakalářskou/diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 19.4.2024 Vladislav Ivančo

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Tomáš Svoboda, Ph.D. za metodické vedení práce a podporující přístup. Pan Svoboda vedl se mnou pravidelné konzultace, které přinášely stálý postup a plně vysvětlující zpětnou vazbu. Chtěl bych mu hlavně poděkovat za náklonost a vřelost, ať už ve formě pravidelných konzultací, zpětné vazby nebo obecnému nasměrování v pokračování bakalářské práce.

Anotace

Bakalářská práce se zabývá tématikou operačních systémů a jejich zabezpečení.

Cílem teoretické části je představit problematiku operačních systémů běžnému uživateli. Jedná se o vysvětlení fungování operačních systémů, představení různých typů, jejich bohaté historie, principů bezpečnosti a využití těchto principů v současných operačních systémech. Pojmy, které jsou spjaté s bezpečností operačních systémů, jsou zde podrobně vysvětleny. Důraz se hlavně klade na pojmy tykající se kybernetické bezpečnosti jako jsou bezpečnostní hrozby, parametry ochrany dat a hardeningová pravidla.

Praktická část prezentuje praktické využití hardeningu na platformě Microsoft Windows. Pro tuto část byl použit software VirtualBox k nasimulování infrastruktury virtuální společnosti. Tato část detailně popisuje veškerou konfiguraci a ověření infrastruktury s případy užití za účelem minimalizace zneužití zranitelností a tím zajištění bezpečnosti operačního systému Windows.

Annotation

Title: Operating systems hardening

The bachelor thesis deals with the topic of operating systems and their security.

The aim of the theoretical part is to introduce the issue of operating systems to the common user. It is an explanation of the functioning of operating systems, introduction of different types, their rich history, security principles and the use of these principles in current operating systems. The concepts that are related to the security of operating systems are explained in detail. Emphasis is mainly placed on concepts related to cyber security such as security threats, data protection parameters and hardening rules.

The practical part presents the practical use of hardening on the Microsoft Windows platform. For this part, VirtualBox software was used to simulate the infrastructure of a virtual company. This section details all the configuration and validation of the infrastructure with use cases to minimize the exploitation of vulnerabilities and thus ensure the security of the Windows operating system.

Obsah

Seznam obrázků

1 Úvod

Tato bakalářská práce na téma „Hardening operačních systémů“ má za cíl představit komplexnost současných operačních systémů s počtem rostoucích bezpečnostních rizik.

K pochopení bezpečnostních rizik a jejich opatření je nejdříve nutné se podívat do světa operačních systémů. Operační systém není pouze pojem, ale velmi složité programové vybavení, které vykonává různé funkce. Mezi tyto funkce patří řízení procesů, správa paměti, správa souborového systému, správa zařízení a ochrana. Každý operační systém tyto funkce zpracovává odlišně, což byl jeden z důvodů pro rozšíření palety typů operačních systémů. Všechny operační systémy mají svůj účel a svoji preferovanou kategorii uživatelů. Tyto účely se zdokonalovaly po dobu několika generací vývoje. Každá generace přinesla něco nového a rozšířila obzory vývoje operačních systému.

Bezpečnost, stejně jako operační systémy, je široký pojem, který zahrnuje více, než se na první pohled zdá. Účelem bezpečnosti je předcházet nebo být aktuální s bezpečnostními riziky. Cílem je ochránit položky zájmů před odcizením nebo nechtěnou změnou. Ovšem i bezpečnost se musí řídit určitými principy, mezi které patří důvěrnost, integrita a dostupnost. Na těchto bezpečnostních principech je postavena CIA triáda, která specifikuje řízení zásad bezpečnosti informací. S postupem času a s příchodem nových technologií byla tato triáda byla rozšířena o další položky, které rozšiřují základní bezpečnostní principy. Vlastnictví rozšiřuje důvěrnost, integrita je rozšířena o autenticitu a užitečnost doplňuje dostupnost. Toto rozšíření vedlo k Parkerian Hexad modelům.

Tyto bezpečnostní principy jsou následně uplatňovány v praxi, kde je velmi důležité uznání a identifikace kybernetických hrozeb. V moderním světě existuje několik kybernetických hrozeb, které se stále zdokonalují a rozšiřují. Proti těmto hrozbám je důležité být připraven ve všech směrech. Nejedná se pouze o opatření, ale i bezpečnostní metody, které mohou danou kybernetickou hrozbu odstranit nebo vyvrátit její dopad. Nicméně největším bezpečnostním rizikem je a bude vždy člověk. Právě proto je potřeba uplatňovat bezpečnostní metody, které omezí nepovolaným uživatelům přístup k citlivým informacím, ať už k systémovým

hodnotám nebo personálním údajům. V těch případech se uplatňují na platformě Microsoft Windows objekty zásad skupiny. Je dobré znát principy fungování a různé typy objektů zásad skupiny a jejich benefity i limity.

Pro představení uplatnění bezpečnostních zásad v praxi provádí tato bakalářská práce čtenáře kompletním a důkladným popisem přípravy. Od samotné instalace virtuálních strojů až po konkrétní případy užití bude uživatel seznámen s praktickými postupy a reálnými případy.

2 Cíl práce

Cílem teoretické části bude seznámit čtenáře s problematikou operačních systémů. Bude důležité pochopit podstatu operačních systémů, jejich funkce, různé typy a historii. Důraz bude kladen na vysvětlení pojmů, jako jsou kybernetické hrozby, jejich opatření, bezpečnostní metody a objekty zásad skupiny.

Praktická část bude mít za úkol představit podrobný postup vybudování virtuální firemní infrastruktury na platformě Microsoft Windows. Postup se bude skládat z kompletní konfigurace Windows Serveru a Windows klienta v softwaru pro virtuální stroje VirtualBox. Kromě konfigurace budou reprezentovány různé případy užití a jejich účel spolu s postupem jejich konfigurace.

3 Teoretické řešení – Operační systémy

Pro hlubší pohled do problematiky operačních systémů si nejprve představíme základní definici a účel operačního systému.

3.1 Operační systém definice

Operační systém je základní programové vybavení sloužící k ovládání hardwarových prvků skrze softwarovou interakci uživatele.

3.2 Základní funkce OS

Pokud není uvedeno jinak, vychází text následující kapitoly ze zdroje [1].

Operační systém vykonává spoustu různých funkcí, ať už na popředí nebo na pozadí. Uživatelé vnímají funkce na popředí, ale to, co se děje na pozadí už jen tak někdo nevidí. A proto si v následujících podkapitolách budou objasněny základní funkce operačních systémů.

3.2.1 Řízení procesů

Řízení procesu je jednou z primárních funkcí operačního systému, která má na starost spravovat a plánovat procesy, případně úlohy, které běží na pozadí operačního systému. Přiděluje jim zdroje procesoru jako jsou čas a paměť pro dosažení efektivního provedení procesu. Zásadními operacemi pro správu procesů je jejich vytváření a ukončování, které umožňují operačnímu systému multitasking a sdílení prostředků mezi různými programy.

Vytvoření procesu

Pro vytvoření nového procesu existuje několik různých způsobu, jak toho dosáhnout:

- Požadavek uživatele – když jako uživatel spustíme aplikaci nebo programovou úlohu, tak operační systém vytvoří nový proces na základě požadavku aplikace nebo programu.
- Inicializace systému – při každém spuštění operačního systému se vytvářejí důležité procesy, které zajišťují plynulý chod operačního systému.

- Vytvoření nadřazeného procesu – v rámci komplexnější aplikace nebo programu, operační systém zpracovává aplikaci nebo program jako hierarchickou strukturu procesu, kde si nadřazený proces vytváří podprocesy pro rychlejší zpracování.

Vytvoření procesu je rozděleno do několika kroků, které se musí správně sekvenčně vykonat:

1. Přidělení Proces Control Block (PCB) – při přiřazení jedinečného identifikátoru novému procesu operačním systémem, je vytvořen řídící blok procesu obsahující informace o procesu, jako jsou jedinečný identifikátor procesu, čítač programu, přidělení paměti a další potřebná data.
2. Přidělení zdrojů – nově vytvořený proces obdrží od operačního systému potřebné prostředky, včetně paměťového prostoru, popisovače souborů a dalších nezbytných prostředků.
3. Nastavení prostředí pro provádění – operační systém nastaví počáteční prostředí pro provádění procesu a společně s tím nastaví čítač programu na startovací bod programu.
4. Načtení programu do paměti – operační systém načte kód programu a jeho data do paměti, a připraví jej ke spuštění.
5. Zahájení provádění – jako poslední krok operační systém spustí provádění nově vytvořeného procesu, který začne vykonávat své instrukce.

Ukončení procesu

Aby ukončení procesu proběhlo správně je potřeba proces řádně ukončit a odstranit ho ze systému. Ukončení procesu může být dosáhnuto několika způsoby:

- Klasické ukončení – po správném vykonání procesu, může dojít k jeho samostatnému ukončení. Proces oznámí své úspěšné ukončení operačnímu systému, který provede nezbytné úkony čištění ke kompletnímu odstranění procesu ze systému.
- Chyba nebo výjimka – v případě naražení na chybu nebo výjimku, kterou nelze opravit, může dojít k neobvyklému předčasnému ukončení procesu.

Operační systém se následně postará o ukončení a provede příslušné ošetření chyb.

- Ukončení nadřazeného procesu – pokud dojde k ukončení nadřazeného procesu, tak v rámci dominového efektu budou i všechny podřazené procesy ukončeny.

I ukončení procesu se řídí určitým postupem, který se musí dobře vykonat, aby byl proces řádně ukončen:

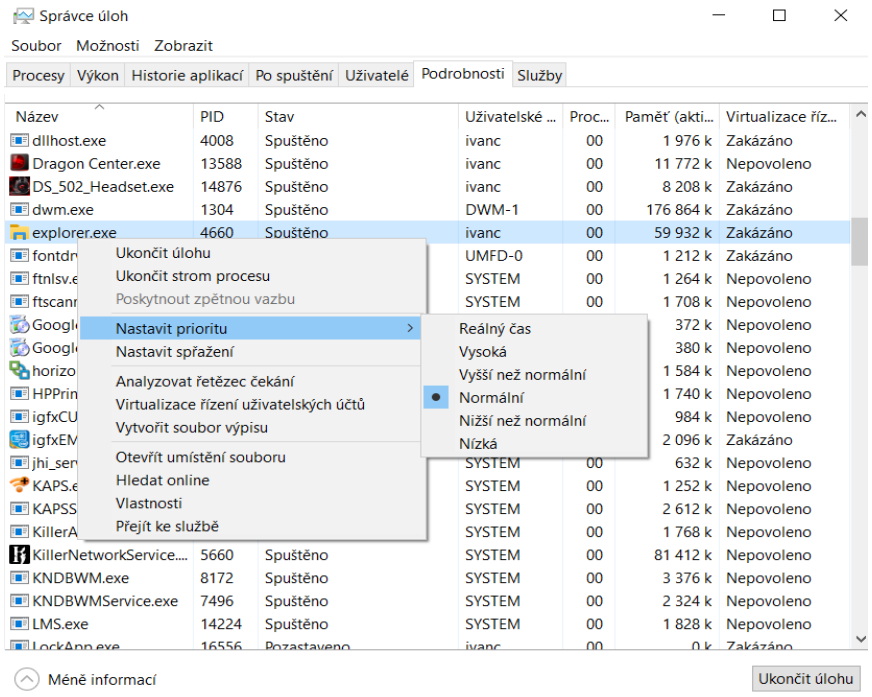
- Provedení úklidu – uvolnění všech prostředků, které byly přiřazeny procesu, zajišťuje, aby nedocházelo k únikům paměti nebo neshodě zdrojů.
- Aktualizace stavu procesu – řídící blok procesu se aktualizuje na stav ukončený a tím je znázorněné, že proces již není aktivní.
- Upozornění nadřazeného procesu – pokud podřazený proces chce být ukončen, musí operační systém informovat nadřazený proces o jeho ukončení. To následně umožní nadřazenému procesu provést potřebné čištění nebo jiné akce.
- Odstranění procesu ze systému – operační systém odstraní ukončený proces ze své tabulky procesů, čímž uvolní systémové prostředky pro jiné procesy.

Plánování procesů

Správa procesu zahrnuje, pro dosažení nejlepší efektivity systému, klíčový prvek plánování procesů. To se stará o určení pořadí procesů na procesoru, kdy se spustí a jak dlouho mohou být spuštěné. Aby bylo možné dosáhnout nejlepší efektivity systému, musí se spravedlivě rozdělit zdroje systému. Na tyto cíle nám slouží algoritmus plánování procesů, který rozhoduje, jak budou procesy spuštěny ze zásoby připravených procesů. Avšak takový algoritmus by nemohl být připraven na všechny případy a poradit si se všemi faktory, proto existuje několik typů algoritmů pro různá zpracování:

- First In, First Out (FIFO) - jedná se o algoritmus typu fronty, což znamená proces, který přišel jako první, bude zpracován jako první. Když proces začne běžet, bude pokračovat, dokud neskončí.

- Shortest Job First (SJF) – podle názvu je jasné, že jsou procesy řazené podle doby provádění. Cílem je minimalizovat čekací dobu a rychlejší zpracování kratších procesů.
- Round Robin (RR) – jedná se o preemptivní algoritmus, kde jsou procesy přepínány v cyklu, aby dostaly přístup k procesoru v určeném pořadí.
- Prioritní plánování – každý proces má nějakou prioritu zpracování, podle které se zpracovává. Priorita může být přiřazena automaticky, podle typu úlohy nebo naléhavosti termínu zpracování, nebo manuálně uživatelem.



Obrázek 1 – Nastavení priority procesu. Zdroj: vlastní

- Víceúrovňové plánování front – procesy jsou zde uspořádány do různých front, s každou frontou používající odlišný plánovací algoritmus. Nejprve jsou naplánovány procesy v rámci svých příslušných front a následně plánovač rozhoduje, jak rovnoměrně rozdělit čas procesoru mezi jednotlivé fronty.
- Víceúrovňové plánování front se zpětnou vazbou – jedná se o rozšířený algoritmus Víceúrovňové plánování front, který umožňuje procesům přecházet mezi různými frontami na základě jejich provádění a využití procesoru. Procesy, které vyžadují výrazné množství procesorového času,

mohou být přesunuty do fronty s nižší prioritou, zatímco procesy s náročnými vstupy a výstupy mohou být přesunuty do fronty s vyšší prioritou.

Synchronizace procesů

Synchronizace procesů zajišťuje správný a uspořádaný přistup více procesů nebo vláken ke sdíleným prostředkům při současném přístupu. Hlavním konceptem synchronizace procesů je předejít různým konfliktům, jako jsou řídící podmínky a nekonzistence dat, které mohou vzniknout při současném přístupu více procesů ke sdíleným prostředkům. Správnou synchronizací lze dosáhnout zvýšení spolehlivosti operačního systému. A právě pro udržení efektivní synchronizace se musí používat vhodné synchronizační mechanismy, které koordinují své akce, vyhýbají se konfliktům a udržují integritu dat:

- Vzájemné vyloučení – zajišťuje, že sdílený prostředek bude dostupný pouze jednomu procesu v daný okamžik. K tomuto nám slouží synchronizační primitiva jako jsou zámky, semafory a mutexy. Princip spočívá v tom, že proces si uzamkne daný zdroj až do dokončení své operace s ním, a teprve poté ho odemkne pro ostatní procesy.
- Semafory – používají se pro omezení počtu procesů, které mohou současně přistupovat k určitému zdroji, nebo pro synchronizaci procesů pomocí blokování nebo odblokování na základě hodnoty semaforu. Tato hodnota je udržena semaforem a může být procesy inkrementována nebo dekrementována.
- Mutexy – umožňují procesu získat exkluzivní přistup k prostředku jeho uzamčení. Po dobu uzamčení mutexem nemohou ostatní procesy přistupovat k prostředku, dokud není uvolněn.
- Proměnné podmínky – na základě jejich vyhodnocení je řízená koordinace více procesů, dokud není podmínka splněna, procesy čekají na oznámení od jiných procesů až podmínka bude splněna.
- Monitory – jedná se o synchronizační konstrukce vyšší úrovně, které kombinují vzájemné vyloučení, proměnné podmínky a sdílené datové

struktury. Data a související operace procesů jsou zapouzdřeny do objektu monitoru, který poskytuje strukturovaný přístup k synchronizaci procesů. Pro zajištění vzájemného vyloučení a synchronizaci, procesy přistupují ke sdíleným datům a volají procesy monitoru.

Deadlock

Deadlock v operačním systému může nastat, když dva nebo více procesů nemohou pokračovat ve svém zpracování, protože každý z nich čeká na uvolnění prostředku, který je držen jiným procesem ve stejné řadě. Tím pádem ani jeden z procesů nemůže pokračovat ve svém konání.

3.2.2 Správa paměti

Správa paměti slouží pro zajištění efektivního přidělení paměti, ochrany procesů před vzájemným zasahováním do paměťového prostoru a maximalizace výkonu operačního systému. Programy a aplikace během svého provádění využívají paměť jako úložný prostor. Z toho důvodu je důležitá efektivní správa a optimalizace paměti spolu s přidělovanými zdroji, aby se předešlo problémům jako jsou úniky paměti, nadměrná fragmentace a nedostatek paměti pro procesy nebo datové struktury.

Virtuální paměť

Virtuální paměť je klíčovým prvkem pro efektivní provádění rozsáhlých programů. Tato technika umožňuje procesům přistupovat k většímu množství paměti, než jaké je fyzicky dostupné v operačním systému. Základním principem je rozdělení logického adresového prostoru procesu do menších jednotek – stránek. Ty jsou poté mapovány do fyzické paměti nebo sekundárního úložiště, jako je pevný disk. Když proces přistupuje k určitému místu v paměti, operační systém pomocí tabulky stránek převádí virtuální adresu na adekvátní fyzickou adresu.

Přidělování paměti

Přidělování paměti probíhá rozdělením dostupné paměti na segmenty, které jsou následně přiděleny operačnímu systému, běžícím procesům a datovým strukturám. Paměť se přiděluje dvěma hlavními způsoby:

- Statické přidělování paměti – spočívá v přidělení paměti procesům nebo datovým strukturám při inicializaci systému, kdy je velikost a umístění paměti předurčené. Tato metoda se používá pro globální proměnné, konstanty a staticky alokované datové struktury.
- Dynamické přidělování paměti – přidělování paměti probíhá za běhu procesů nebo datových struktur dle požadavků programu, které mohou dynamicky požadovat a uvolňovat paměť. To je zajištěné prostřednictvím různých algoritmů přidělování paměti:
    - First-Fit
    - Best-Fit
    - Worst-Fit
    - Next-Fit

V rámci rozdělení paměti, ji také můžeme rozdělit na menší nesouvislé bloky pomocí operací alokace a dealokace paměti – fragmentace. Tu následně můžeme rozdělit na dva typy:

- Externí fragmentace – dochází k ní, když volné bloky paměti jsou rozházené po celém operačním systému. Proto je složitější přidělit procesu souvislé bloky paměti, i když je celkový objem volné paměti dostatečný.
- Interní fragmentace – je způsobena velikostí alokovaných bloků, které jsou větší, něž jejich data uvnitř. To vede k plýtvání paměti v rámci alokovaných bloků.

Ochrana paměti

Ochrana paměti zajišťuje izolaci a bezpečnost procesů tím, že brání neoprávněnému přístupu k paměťovým adresám a jejich neautorizované modifikaci. Hlavním cílem je zabránění vzájemného zasahování procesů

do paměťového prostoru mimo přidělené segmenty a zachování stability a integrity operačního systému. Uplatněním kontroly přístupu a využívání metod pro správu paměti poskytují operační systémy robustní rámec pro ochranu paměti v moderních počítačových prostředích. Pro příklad si uvedeme důležité vlastnosti a techniky ochrany paměti:

- Segmentace paměti – rozděluje adresní prostor do logických segmentů, přičemž každý segment představuje samostatnou část paměti procesu. Použitím segmentace se zajistí, že různé části procesu mají rozdílná přístupová práva.
- Řízení přístupu – určuje přístupová práva k určitým segmentům paměti, jako jsou práva pouze pro čtení, čtení a zápis nebo ke spuštění. Kdykoliv se proces pokusí připojit k paměťovému umístění, tak operační systém vynutí řízení přístupu pro kontrolu přístupových práv.
- Address Space Layout Randomization (ASLR) – bezpečnostní technika, která náhodně mění rozložení paměti procesu, čímž ztěžuje útočníkům zneužití zranitelností paměti a zvyšuje bezpečnost systému díky snížení předvídatelnosti umístění paměti.
- Výjimky z ochrany paměti – pokud se proces pokusí připojit k paměti, ke které nemá přístupová práva, je vyvolána výjimka z ochrany paměti. Když operační systém tuto výjimku zachytí, provede příslušné akce, jako je ukončení procesu nebo vygenerování chybové zprávy.

3.2.3 Správa souborového systému

Správa souborového systému organizuje, ukládá a načítá data na úložných zařízeních. Zde jsou uvedeny některé klíčové aspekty a funkce souborových systémů, které také zahrnují správu souborů, adresářů a metadata spojených s uloženými daty:

- Organizace souborů – organizace dat do souborů, což jsou logické jednotky informací, které mohou představovat dokumenty, programy, obrázky, videa a další typy dat. Souborové systémy přidělují souborům jméno, úložiště a přístupnost.

- Struktura adresáře – souborové systémy obvykle podporují hierarchickou adresářovou strukturu, která umožňuje soubory a adresáře organizovat do stromového uspořádání.
- Metadata souborů – jsou vázány k souborům a poskytují informace, jako je název souboru, velikost, datum vytvoření, datum změny a oprávnění, což usnadňuje správu a přístup k nim.
- Přístup k souborům a oprávnění – je určen řízením přístupu a oprávněními, která určují, kdo může soubory číst, zapisovat nebo spouštět. Tím se zajistí, že k souborům mohou přistupovat nebo je upravovat pouze oprávnění uživatelé nebo procesy na základě svých oprávnění.
- Alokace souborů – spravuje přidělování a rozdělování úložného prostoru, což slouží pro ukládání souborů. Také zajišťuje efektivní využití dostupného místa na úložišti. Existují různé metody přidělování:
    - Souvislé přidělování
    - Vázané přidělování
    - Indexované přidělování
- Integrita souborového systému – pro zachování integrity uložených dat existují mechanismy, jako jsou žurnálování nebo transakční aktualizace, které pomáhají obnovit systém po selhání nebo výpadku napájení, aniž by hrozilo poškození nebo ztráta dat.
- Operace souborového systému – mezi které patří vytváření, čtení, zápis, mazání a úprava souborů jsou prováděny přes systémová volání nebo API, které spojují aplikace a operační systém se souborovým systémem.

Existují různé souborové systémy, které mají různé funkce, výkonnostní popis a kompatibilitu s různými operačními systémy. Mezi ty nejznámější patří:

- FAT (File Allocation Table)
- NTFS (New Technology File System)
- HFS+ (Hierarchical File System Plus)
- ext4 (Fourth Extended File System)
- APFS (Apple File System)

3.2.4 Správa zařízení

Správa zařízení koordinuje vstupní a výstupní operace mezi softwarem a hardwarem. Vstupem je forma dat nebo signálů přijatých softwarem z hardwaru, zatímco výstupem se rozumí data nebo signály odeslané ze softwaru do hardwaru. Operační systém zahrnuje ovladače zařízení, což přispívá k hlavnímu cíli správy zařízení. Mezi tyto cíle náleží zpracování dat nebo signálů, zajištění integrity dat a optimalizace výkonu operačního systému.

Ovladače zařízení

Ovladače zařízení jsou softwarové programy, které poskytují konzistentní a standardizované rozhraní pro interakci operačního systému s hardwarovými zařízeními. Slouží jako prostředníci a operační systém přes ně odesílá příkazy a přijímá data. Ovladače zařízení jsou obvykle vyvíjeny a udržovány výrobci hardwaru a jsou specifické pro každé hardwarové zařízení. Mezi několik důležitých funkcí a vlastností ovladačů zařízení patří:

- Hardwarové rozhraní – poskytnuté ovladačem zařízení slouží jako abstraktní vrstva pro lepší komunikaci mezi operačním systémem a širší škálou hardwarových zařízení, aniž by operační systém musel rozumět specifikům jednotlivých zařízení.
- Inicializace zařízení – když dojde k připojení hardwarového zařízení k počítači, ovladač zařízení provede inicializaci a konfiguraci zařízení. To zahrnuje detekci zařízení, nastavení potřebných hardwarových parametrů, přidělení systémových prostředků a přípravu zařízení k provozu. Dnes je to řešeno technologií plug-and-play.
- Ovládání zařízení – umožňuje operačnímu systému řídit a spravovat operace hardwarových zařízení, jako je otevírání a zavírání připojení k zařízení, čtení ze zařízení a zápis do zařízení, nastavení parametrů zařízení a zpracování určitých příkazů pro zařízení.
- Obsluha přerušení – zpracovává generovaná přerušení hardwarových zařízení a upozorňuje na ně operační systém, který na ně může vhodně reagovat.

- Zpracování chyb – zjišťuje a hlásí chyby, které musí být následně zpracovány pomocí mechanismů obnovy chyb, aby zajistily další provoz zařízení.
- Optimalizace výkonu – je dosažena ovladači zařízení, které implementují vyrovnávající paměť, mezipaměť a kompresi dat, což vede ke zlepšení rychlosti přenosu dat a snížení latence.

3.3 Představení různých OS – Windows, OS X a Linux

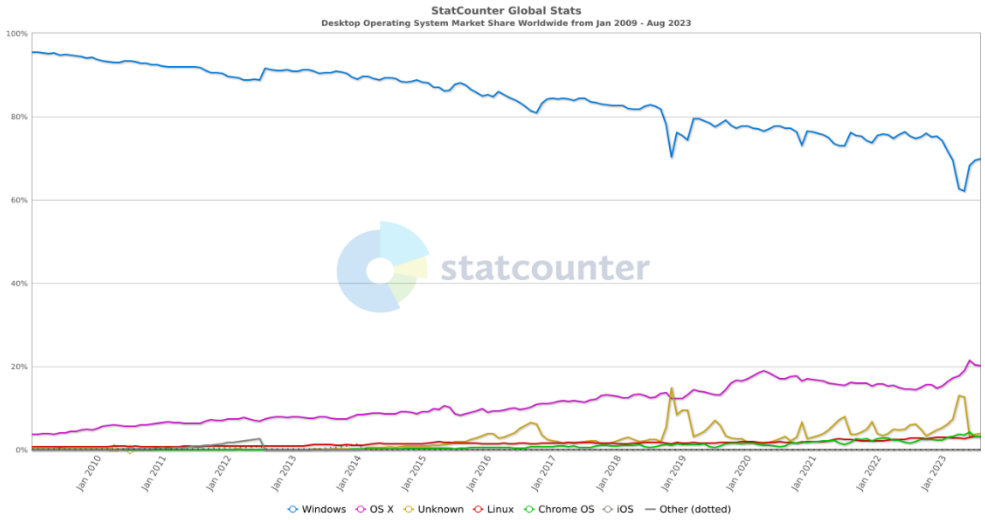
Pokud není uvedeno jinak, vychází text následující kapitoly ze zdroje [3].

V následujících kapitolách se seznámíme s různými operačními systémy, jejich dlouholetou historií a vývojem. Hlavním zaměřením bude bezpečnost – proč je důležité se jí věnovat, jaké prostředky nám pomáhají ji udržovat, například antivirové programy a skupinová politika ve firmách, a obecně základy zabezpečení.

V průběhu několika let technologie zaznamenaly velký pokrok. My jakožto lidstvo máme schopnost realizovat své cíle, avšak ne vždy tou nejpoctivější cestou. I v oblasti operačních systémů se vývoj odvíjel podobně. Motivací pro vývoj nových operačních systémů bylo hledání nových možností a inovací. Avšak ani soutěživý prvek zde nebyl zanedbán. Jehož presence sehrála tak velkou roli, že díky ní máme na výběr hned z několika operačních systémů. Ale co vedlo k zdokonalení těchto různých operačních systému, byly uživatelské preference. Právě tyto preference určují směr vývoje a inovací.

Během celého časového zdokonalovaní je na první pohled patrné, že operační systém od firmy Microsoft je stálým vedoucím desktopovým klenotem

mezi operačními systémy. Obrázek 2 reprezentuje fakt, že ostatní systémy mají lepší nárůst popularity než gigant od Microsoftu. [2, 3]



Obrázek 2 - Popularita operačních systémů. Zdroj: [2]

V následujících kapitolách se budeme věnovat třem hlavním operačním systémům v tomto pořadí:

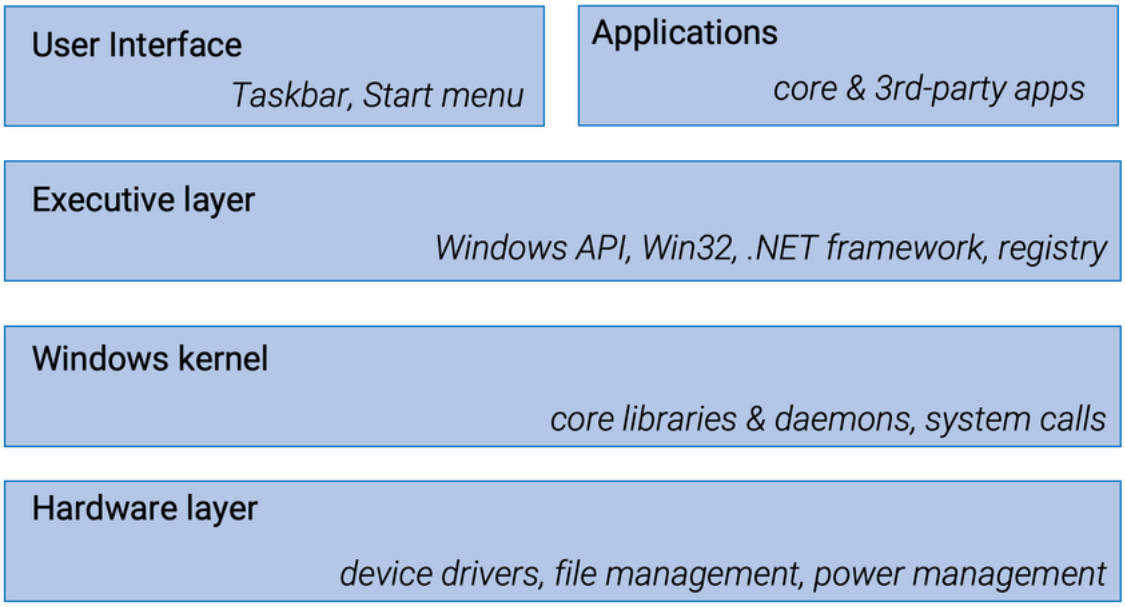
- Windows
- OS X
- Linux

3.3.1 Windows

Původně byl operační systém od firmy Microsoft navržen jako grafické uživatelské rozhraní nad systémem MS-DOS. K přechodu na dnes populární operační systém Windows vedla integrace všech systémových funkcí MS-DOS do verze Windows 95, která se stala velice úspěšnou. Do pole úspěšnosti patří i vrstvená architektura zachovaná ve Windows. Obrázek 3 ukazuje každou vrstvu i s vlastní sadou služeb:

- Hardwarová vrstva – přistupuje k hardwarovým zařízením počítače jako jsou procesor, paměti, úložiště a vstupně-výstupní periferie.
- Vrstva jádra – je zodpovědná za základní služby operačního systému, jako jsou řízení procesů, správa paměti, správa souborového systému a správa zařízení.

- Výkonná vrstva – poskytuje sadu služeb nad jádrem, včetně rozhraní API operačního systému Windows a subsystémů pro spuštění aplikací, jako je subsystém Win32 a framework .NET. Jako hlavní databáze systému Windows, určená k ukládání všech nastavení počítače, slouží registru systému. Registr obsahuje uživatelské informace týkající se hesel a zařízení. Pro zobrazení těchto informací existuje Editor registru, který zobrazuje všechny klíče, hodnoty a dokonce i ovladače zařízení.
- Grafické uživatelské rozhraní (GUI) – zpracovává komunikaci mezi uživatelem a počítačem. Grafické uživatelské rozhraní systému Windows se stalo zřetelně oddělenou vrstvou až ve verzi Windows 8. Avšak už Windows XP představil některé základní grafické prvky rozhraní jako je nabídka Start, hlavní panel, systémová lišta a průzkumník oken.



Obrázek 3 - Základní architektura vrstev ve Windows. Zdroj: [3]

Pro správu operačního systému Windows lze využít vlastní terminál v podobě příkazového řádku. Avšak pokud by byly potřeba rozsáhlejší funkce, je k dispozici PowerShell, který nabízí výkonné možnosti skriptování. Při ukládání souborů operační systém Windows spoléhá na adresářovou strukturu, jejíž původ lze vystopovat až k systému MS-DOS. Soubory lze následně ukládat do adresářové struktury – složky nebo je mazat, kde se místo složek objeví v koši. Operační systém Windows také obsahuje spoustu vestavěných bezpečnostních funkcí, jako je Řízení uživatelských účtů a antivirový program Windows Defender. Tyto funkce jsou

integrovány do jádra a výkonné vrstvy operačního systému a rovněž poskytují sadu rozhraní API pro vývoj bezpečných aplikací.

3.3.2 OS X

Proprietární operační systém od společnosti Apple je známý svým snadným používáním, elegantním designem a integrací s dalšími zařízeními a službami Apple. OS X je v současnosti založen na unixovém operačním systému, podobně jako operační systém Linux. Využívá hybridní architekturu jádra, která umožňuje poskytovat některé služby jádra v uživatelském prostoru, zatímco jiné v prostoru jádra. Tím je dosažena rovnováha mezi výkonem a zabezpečením. Jádro jako takové poskytuje základní služby operačního systému, mezi které patří řízení procesů, správa paměti a správa zařízení.

Jedinečné rozhraní Aqua poskytuje OS X elegantní a intuitivní grafické uživatelské rozhraní, které obsahuje spoustu vestavěných aplikací. OS X poskytuje shell unixového typu, a stejně tak je zde stále k dispozici i Bash. Avšak po aktualizaci Catalina je nastaven jako výchozí shell Z-shell.

Souborový systém je zde řešen typickou stromovou unixovou strukturou s adresáři specifickými pro OS X, které obsahují specifika architektury počítače od Applu. Pro příklad ve složkách Preferences se nacházejí soubory typu *.plist, ve kterých jsou uložena všechna nastavení vlastností aplikací.

Jedinečnými bezpečnostními funkcemi zde jsou funkce Gatekeeper, který omezuje instalaci z neznámých zdrojů, a funkce FileVault, který zajišťuje šifrování celého disku.

OS X se stal značně oblíbenou volbou mezi kreativními tvůrci, díky své architektuře a snadnému propojení s ostatními produkty od společnosti Apple.

3.3.3 Linux

Linux je operační systém s otevřeným zdrojovým kódem a každý si ho může přizpůsobit podle svého použití. Toto přizpůsobení je umožněno faktem, že Linux je vydán pod licencí GNU General Public License (GPL). Je založený na operačním systému Unix a původně byl určen pro vývojáře GNU. Používá se na široké škále zařízení, od serverů po chytré telefony, a proto existuje spousta volně dostupných

distribucí (např. Ubuntu, CentOS, Debian, Arch Linux, Linux Mint atd.). Avšak ne všechny distribuce jsou volně dostupné, některé z nich jako třeba Red Hat Enterprise Linux (RHEL) jsou schované za platební bránou. Jedná se o stabilní, bezpečný a flexibilní operační systém, který se stal velice univerzální volbou pro každého. [3, 4, 5]

Podobně jako jeho předchůdce využívá modulární architekturu jádra, které je zodpovědné za poskytování základních služeb operačního systému. V rámci modularity už do samotného běžícího jádra lze nahrát části kódu, které rozšiřují funkčnost nebo přidávají podporu nebo funkce pro specifická hardwarová zařízení. Vše je řešeno pomocí modulů Loadable Kernel Modules, které poskytují způsob přidání nových prvků do jádra, aniž by bylo nutné celé jádro přestavovat a nahrazovat. Moduly lze načítat nebo odpojovat podle potřeby, čímž je snížena spotřeba vlastního jádra pro každou konfiguraci, zajištěna větší flexibilita a kompatibilita s širokou škálou hardwarových architektur, jako jsou x86, ARM a MIPS. Kromě modulů Linux obsahuje sadu nástrojů a knihoven uživatelského prostoru, které poskytují další služby, jako je třeba knihovna GNU C.

Linux také obsahuje kromě nástrojů a knihoven mnoho subsystémů a služeb, které jsou postaveny nad jádrem a nástroji uživatelského prostoru. Grafické uživatelské rozhraní je poskytováno X Window System. V něm si lze vybrat z různých desktopových prostředí a správců oken, jako jsou GNOME, KDE nebo XFCE. Terminál se zde nachází v podobě shellu a opět si lze vybrat typ shellu z velké nabídky, avšak tím nejpoužívanějším je Bash. Zvolený shell určuje, jak se terminál chová a vypadá.

V praxi se Linux také používá pro jeho nativní podporu kontejnerizace. Kontejnerové technologie, jako jsou Docker a Kubernetes, využívají řadu Linuxových funkcí, mezi které patří jmenné prostory a skupiny cgroups, které poskytují vzájemnou izolaci procesů a řízení využívání zdrojů.

Linux, na rozdíl od Windows, který spoléhá na samostatné instalační balíčky, používá linuxové distribuce pro správu balíčků, jako je APT nebo YUM, které zjednodušují instalaci softwaru, aktualizace a správu závislostí. I v rámci souborů je Linux odlišný, má vlastní kódovou základnu, která ukládá data jako jediný strom souborů, na kterém jsou připojeny všechny disky a zařízení. Dokonce tu nenarazíme

na vlastní specifický registr. Všechny konfigurace aplikací jsou ukládány program po programu, pro každého uživatelé zvlášť, ve stejném hierarchickém formátu pro ukládání ostatních souborů. Nenachází se zde žádná centralizovaná databáze pro uložení těchto podrobností.

3.4 Historie OS

Pokud není uvedeno jinak, vychází text následující kapitoly ze zdroje [6].

Jak již bylo řečeno, operační systémy se neustále vyvíjejí a prošly několika změnami, než dostaly podobu, jakou je známá dnes. Jejich vývoj závisí na nových technologiích a jak mohou zlepšit výkon a funkce operačního systému. V následujících podkapitolách bude představena evoluce operačních systémů a jejich vývoj v průběhu času:

3.4.1 Doba bez OS (do 1940 / 0. generace)

Do roku 1940 koncept operačního systému neexistoval, takže každá úloha v počítačovém systému se musela zadávat ručně ve strojovém kódu (jazyk 0 a 1). Realizace těchto úloh byla velice složitá, časově náročná a uživatelsky nepřívětivá. I přes to, že úlohy reprezentovaly jednoduché matematické problémy, mohly být bezproblémově zpracovávány pouze těmi, kteří měli hluboké znalosti strojového kódu. [6, 8]

3.4.2 Systém dávkového zpracování (1940–1950 / 0. a 1. generace)

Pro roce 1940 se s postupem času objevil na trhu systém dávkového zpracování. Uživatelům se otevřela možnost zapisovat programy na děrné štítky a ty načítat do počítače. Různé dávky podobných úloh, které jsou vytvořeny operátorem, jsou postupně předkládány ke zpracování procesoru. Procesor tyto dávky zpracovává sekvenčně. Nejznámější využití tohoto systému bylo anglickým matematikem a počítačovým vědcem Alanem Turingem, označovaným jako „Otcem moderní informatiky.“ Během 2. světové války pomohl prolomit kód Enigma, což vedlo k jejímu rychlejšímu konci. [6, 7]

3.4.3 Víceprogramové systémy (1950-1960 / 1. a 2. generace)

V tomto období začala skutečná revoluce. Děrné štítky byly nahrazeny elektronkami a tranzistory. Tyto systémy pracovaly s dávkami magnetických pásek a mechanik, což zvýšilo efektivitu. Také se objevila možnost načíst více programů do paměti a každému z nich přidělit určitou část paměti. V případě dlouhého zpracování jednoho programu, operační systém povolí procesu přepnout z předchozího programu na jiný, který je první ve frontě připravených programů. Tím je dosaženo plynulého provádění programů s přerušením. Jeden z prvních počítačů těchto systému byl IBM 704, představen výzkumnou divizí General Motors. [6, 7]

3.4.4 Systémy sdílení času (1960-1970 / 2. a 3. generace)

Systémy sdílení času jsou rozšířením systému multiprogramování o jednu velkou funkci. Ta brání dlouhodobému využívání procesu jednotlivými programy a aby při jejich zpracování byl procesor zpřístupněn po určitém časovém intervalu. To funguje tak, že operační systém po určitém časovém intervalu přepne z jednoho programu na druhý, aby každý program mohl získat přístup k procesoru a dokončit svoji úlohu.

3.4.5 Grafické uživatelské rozhraní (1970-1980 / 3,5. generace)

Pro zlepšení uživatelské interakce a přívětivosti přišlo grafické uživatelské rozhraní. Díky němu veškerá interakce mezi uživatelem a počítačem se stala pohodlnější a snadnější. Uživatelům místo psaní příkazů nyní stačilo klikat pouze na vizuální prvky. V rámci operačního systému Windows se jednalo o ikony, nabídky a okna v MS-DOS. Avšak jako první operační systém, co využil grafické uživatelské rozhraní, byl MacOS. [6, 8, 9]

3.4.6 Síťové systémy (1980-1990 / 4. generace)

Síťové systémy posunuly operační systémy o laťku výše. Až natolik, že pro jejich správu bylo zapotřebí vyvinout speciální typ operačních systémů (Windows NT a Novell NetWare). Ty umožnily uživatelům pracovat

ve stejném prostředí v rámci spolupráce a velmi usnadnily sdílení souborů a vzdálený přístup.

4 Bezpečnost

Pokud není uvedeno jinak, vychází text následující kapitoly ze zdroje [10].

Bezpečnost v informačních technologiích je nesmírně široký obor, který zahrnuje mnoho oblastí, od zabezpečení uživatelských dat, až po fyzickou bezpečnost uživatele. A právě proto se týká jak hardwaru a softwaru, tak i sociálního chování uživatelů operačního systému. V rámci počítačového zabezpečení platí, princip nedůvěry. Jsou bezpečné pouze z výpočetního hlediska.

4.1 Účel bezpečnosti

S technologickým pokrokem se množství výpočetních prostředků, které jsou k dispozici pro narušení počítačové bezpečnosti, rok od roku exponenciálně zvyšuje. V důsledku toho je nutné bezpečnostní opatření modernizovat, aby byla zajištěna stejná úroveň bezpečnosti v reálném čase.

4.1.1 Soukromí

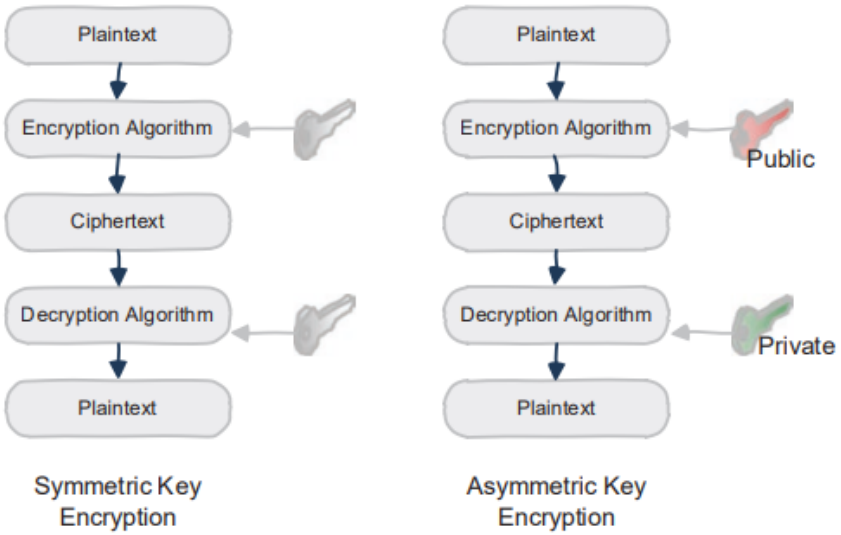
Soukromí je jednou z důležitých oblastí, která je vždy silně spojena s bezpečností. Základní bezpečnostní mechanismy používané k ochraně dat jsou podobné jako mechanismy používané k ochraně soukromí, které se týkají důvěrnosti informací umožňujících osobní identifikaci.

4.1.2 Důvěrnost

V rámci důvěrnosti se zkoumá, zda jsou údaje tajné nebo nikoliv. Pokud si uživatel může jednoduše data zobrazit, považují se za nedůvěryhodná. Avšak pokud je nelze jednoduše zobrazit, jsou důvěryhodná.

Pro zajištění důvěryhodnosti dat se používají šifrovací algoritmy, kterých existuje celá řada. Nezašifrovaná data, nazývaná též plaintext, se posílají přes šifrovací algoritmus, čímž se vytvoří šifrovaný text neboli ciphertext. K šifrování se používá šifrovací klíč, který nese klíčovou informaci k dešifrování nebo šifrování dat. Obrázek 4 představuje šifrovací způsoby a využití šifrovacích

klíčů. V symetrickém šifrování je pro šifrování a dešifrování použit stejný klíč, zatímco v asymetrickém šifrování je pro obě operace použit odlišný šifrovací klíč. [10, 11]



Obrázek 4 - Symetrické a Asymetrické šifrování. Zdroj: [10]

V současné době je nejsilnějším šifrovacím algoritmem AES, který je považován za mnohem bezpečnější než jeho předchůdci DES a 3DES. Většina kryptografických knihoven poskytuje API pro šifrování AES a většina procesorů společností Intel, AMD, Apple a ARM podporuje instrukce pro akceleraci šifrování a dešifrování AES.

Řízení přístupu

Hlavním ze způsobu řešení důvěrnosti dat je řízení přístupu v operačním systému. Řízení přístupu určuje základní bezpečnostní vlastnosti dat:

- Čtení – umožňuje data přečíst, pokud nejsou blokována.
- Zápis – umožňuje zapisovat data v systému, pokud nejsou uzamčená.
- Spuštění – nasměruje uživatele k provedení příkazů.

Vlastnost dat je spíše z pohledu uživatele. Jinak řečeno, různí uživatele mohou mít ke stejným datům jiná přístupová práva a jejich kombinace. V operačním systému jsou tyto bezpečnostní vlastnosti specifikovány softwarem a vynucovány hardwarem. Tím je dosažené řízeného přístupu k datům a je vyžadováno důvěryhodným uživatelem v operačním systému, který vlastní veškerý přístup

k datům. Prerekvizitou pro zajištění důvěrnosti je úspěšná autentizace uživatele do operačního systému nebo aplikace.

V mnoha případech nelze použít řízení přístupu pro získání vlastností dat. Tyto situace si žádají použití kryptografie. Kryptografie, jakožto věda, se zabývá ochranou dat v přítomnosti útočníka.

4.1.3 Integrita

Integrita zajištuje pravost a úplnost dat. Pokud legitimní uživatel může data zapisovat, tak jejich integrita je kontrolována daným uživatelem. Zajištění integrity dat lze dosáhnout zašifrováním symetrickým algoritmem a stejný šifrový text poskytne stejná nešifrovaná data při použití stejného klíče. Zde může nastat problém, když útočník změní šifrovaný text, který nahradí původní nezašifrovaná data. Pro předejití toho problému bylo zavedeno hashování.

Hashování je proces mapování libovolně dlouhého datového blobu na datový blob o fixně dané velikosti neboli hash. Algoritmy hashování jsou jednosměrné funkce, které zaručují, že k dané hodnotě hash nelze najít jiný datový blob se stejnou hodnotou hash po zkomprimování. Při použití stejného algoritmu se vždy daný datový blob bude hashovat na stejnou hodnotu hash. Pro zajištění integrity datového blobu, je hodnota hash chráněna uložením odděleně od datového blobu, nebo zašifrováním. V kryptografii se běžně používají hashovací funkce SHA-3 a SHA-512, které podporují maximálně 512 bitů hashe.

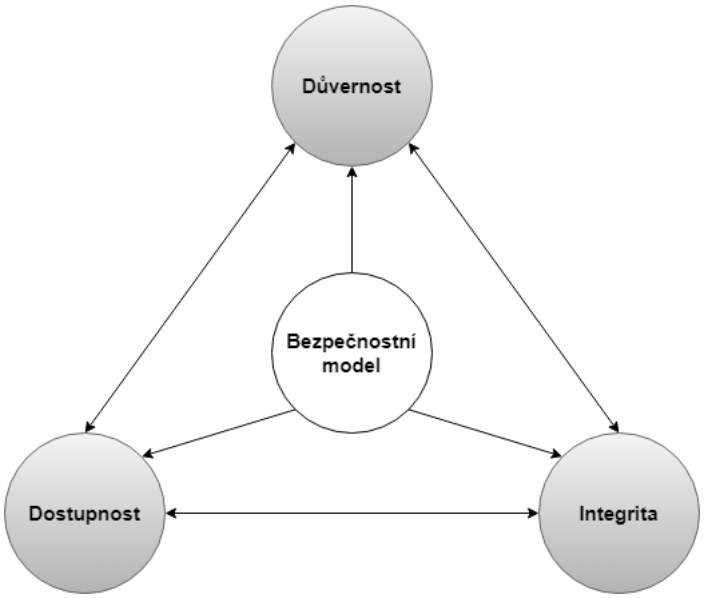
4.1.4 Dostupnost

Dostupnost poukazuje na fyzickou přítomnost dat. Pokud má uživatel přístup k datům a oni se nacházejí ve svém přiřazeném uložišti, považují se za dostupná. Ovšem pokud jsou data ze svého umístění v úložišti či paměti odstraněna nebo přistup k nim je bráněn útočníkem, považují se za nedostupná. Dostupnost dat je zajištěna omezením přístupu útočníka k datům a tím, že operační systém kontroluje mazání dat.

4.1.5 CIA triáda

Pokud není uvedeno jinak, vychází text následující kapitoly ze zdroje [12].

CIA triáda zastupuje předešlé principy bezpečnosti (důvěrnost, integritu a dostupnost) v podobě modelu určeného k řízení zásad bezpečnosti informací. Zkratka modelu se občas zaměňuje za AIC triádu pro předejití záměny s Ústřední zpravodajskou službou (CIA). Důvěrnost v modelu je rozsáhlým souborem pravidel, která omezují přístup ke všem typům dat a informací. Přesné a důvěryhodné informace jsou zárukou integrity. Forma řízení rizik je dostupnost, které má poskytnout spolehlivý přístup oprávněným osobám k těmto datům a informacím. Tyto principy jsou vodítka pro tvorbu bezpečnostních politik organizací, nad kterými by se mělo přemýšlet jako o vzájemně propojeném systému, nikoliv jako o samostatných konceptech. CIA triáda pomáhá zohledňovat poskytované hodnoty v těchto principech při vyhodnocování potřeb a použití nových technologií.



Obrázek 5 – Model CIA triády. Zdroj: vlastní. Upraveno dle [13]

Model CIA triády přináší spoustu výhod řadě podnikům, které pracují s citlivými udají:

- Bezpečnost dat a ochrana soukromí – jsou nezbytné před dnešními sofistikovanými kybernetickými útoky a dalšími neoprávněnými pokusy o přístup k cenným informacím, jejich manipulaci nebo odcizení.
- Dodržování předpisů – pro zajištění důvěrnosti, integrity a dostupnosti citlivých informací.

- Proaktivní prevence rizik – je dosáhnutá v prostředí, které je vytvořeno správnou aplikací CIA triády. Stávající zranitelnosti jsou identifikovány a zmírňovány, aby se zabránilo budoucím hrozbám.
- Komplexnost – spočívá v použití všech prvků CIA triády. Nejedná se pouze o zmaření útočníků, ale i o zajištění pravdivosti a dostupnosti dat.

Navzdory výhodám CIA triády mohou být při její implementaci také výzvy a nevýhody:

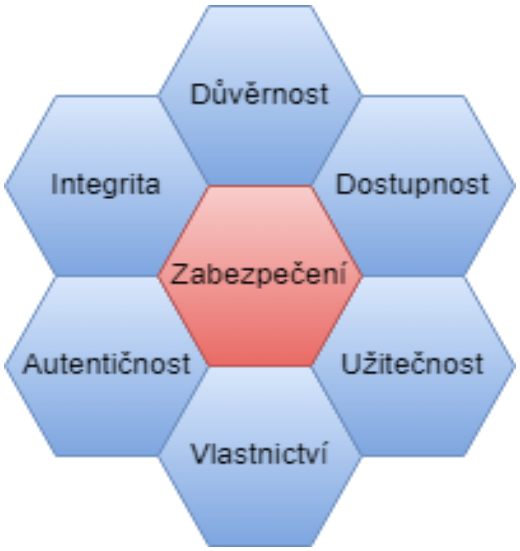
- Velké datové objemy – představují pro paradigma CIA výzvu kvůli obrovskému objemu informací, mnoha zdrojům a různým formátům, které je potřeba ochránit.
- Odpovědná správa a řízení dat – často chybí kvůli shromažďování velkých dat a jejich užitečné interpretaci.
- Bezpečnost a soukromí internetu věcí (IoT) – jsou důležitými aspekty, protože údaje posílané internetem věcí mohou představovat bezpečnostní riziko pro soukromí. Obzvlášť, když jsou data shromažďovány, analyzovány a porovnávány z různých zařízení.
- Zabezpečení při vývoji produktů – je důležité zvažovat, protože se vyvíjí stále více produktů s možností připojení k síti.

4.1.6 Parkerian Hexad modely

Pokud není uvedeno jinak, vychází text následující kapitoly ze zdroje [13].

Představení Parkerian Hexad modelů vedlo ke zdokonalení a lepšímu chápání informační bezpečnosti, protože se dostatečně nesoustředilo na uživatele při udržování a obraně proti ztrátám souvisejícími s informacemi. Rozšíření CIA triády bylo nejlépe pochopeno a implementováno, když byly jednotlivé principy seskupeny dohromady. Navrhlo se, aby se na jednotlivé principy pohlíželo v následujících skupinách:

- Důvěrnost a vlastnictví
- Integrita a autenticita
- Dostupnost a užitečnost



Obrázek 6 – Model Parkerian Hexad. Zdroj: vlastní. Upraveno dle [13]

Každé porušení důvěrnosti je porušením vlastnictví, avšak obráceně to neplatí. V bezpečnosti informací musí být více zohledňován lidský faktor. Data by měla být důvěrná, ale také musí být zajištěna jejich oprávněná manipulace. Porušování autorských práv není zahrnuto v rámci zájmů CIA triády. Otevřená a veřejná data je stále potřeba chránit. Pokud se někdo rozhodne znovu použít kopírovaný písemný materiál, musí existovat způsob, jak porušení definovat. Jeden z příkladů, že CIA triáda nezahrnuje dostatečný zásah uživatele.

K porušení integrity dochází při neoprávněné změně dat, ať už úmyslné nebo náhodné. Integrita silně spoléhá na technologii oproti lidskému prvku. Kontrola cyklické redundance a hashovací algoritmy jsou přínosné, ale už neberou v potaz autentičnost dat. Autenticita zaručuje, že daná data pochází ze zdroje, za který se vydává, to může být dosaženo důkazem o totožnosti. CIA triáda tento důležitý prvek přehlíží.

Při dostupnosti dat se musí posuzovat, zda jsou v použitelném nebo korektním stavu. Pro zajištění dostupnosti se implementuje redundance, převzetí služeb při selhání a clustery. Dostupnost neřeší použitelnost výstupů. Použitelnost se hlavně zaměřuje na obsah dat a díky jejich složitosti se stala ještě

důležitější. CIA triáda tento koncept kontextově přehlíží, a právě proto jsou Parkerian Hexad modely komplexnější a úplnější.

5 Bezpečnost v OS

Pokud není uvedeno jinak, vychází text následující kapitoly ze zdroje [14].

Klíčovou roli při ochraně operačního systému a dat před kybernetickými hrozbami a neoprávněnými uživateli hraje zabezpečení operačního systému. Bezpečnost operačního systému zajišťuje ochranu souborového systému a integritu dat. Procesy, které jsou zpracovány současně, by měly být od sebe oddělené operačním systémem, aby bylo zajištěno integrity aplikací a ochrany před možným rušením a útoku ze strany jiných procesů. Pro tyto situace jsou v operačním systému abstraktní konstrukce, jako jsou procesy spojené s bloky řízení úloh, virtuální paměťové prostory, soubory, porty a komunikace mezi procesy. Integrita v operačním systému je dosažena omezením neoprávněného přístupu a nežádaných operací prováděných nad daty. Oprávněný přístup je udělen uživateli na základě identity, vlastnictví uživatele a autorizace. [14, 15]

5.1 Kybernetické hrozby

Jak již bylo řečeno, operační systém Windows je nejrozšířenějším operačním systémem na světě, a právě proto je nejvíce cílen k prolomení. Kybernetické útoky nejčastěji využívají internetového připojení k infikování cílového zařízení. V rámci internetového připojení se kybernetické útoky šíří řadou kanálů, včetně phishingových emailů, infikovaných webových stránek, přenosných medií, softwaru staženého z pochybných zdrojů i využitím bezpečnostních chyb v operačním systému a softwaru. Rozlišujeme několik kybernetických hrozeb, avšak jakýkoliv program nebo kód určený k narušení, poškození nebo získání neoprávněného přístupu k operačnímu systému nebo síti označujeme jako škodlivý software neboli malware. K vytvoření malwaru se používají různé nástroje jako jsou viry, červi, trojské koně, spyware, adware a mnoho dalších. Hlavním cílem kyberzločinců je získat přístup k systémovým prostředkům a neoprávněně je používat. Po úspěšném napadení operačního systému nebo počítačové sítě dochází k řadě problémů. Mezi tyto problémy patří ztráta dat, financí, poruchy operačního systému,

neoprávněný přístup, krádeže identity a porušení soukromí. Existuje několik typů malwaru, ale mezi ty používanější patří [14, 16]:

- Rootkity – pracují v režimu jádra a mají stejná oprávnění jako operační systém. Mohou se v operačním systému ukrývat libovolně dlouho. Po jejich použití se informace o zařízení stávají nedůvěryhodnými. Níže jsou uvedeny čtyři nejčastější rootkity:
    - Firmwarové rootkity – přepisují firmware zařízení, aby se spustily dříve než operační systém.
    - Bootkity – jsou rozvinuty o schopnost napadnout hlavní zaváděcí záznam a zůstávají aktivním během jeho použití.
    - Rootkity jádra – získávají přístup k jádru operačního systému a následně nahrazují jeho část, aby po spuštění operačního systému byly aktivní.
    - Rootkity ovladačů – se vážou na ovladače zařízení, protože ty pracují v režimu jádra, takže mají přístup ke všem důležitým souborům v operačním systému.
- Phishing – využívá e-maily, textové zprávy, webové stránky a další typy elektronického připojení ke krádeží soukromých informací. Jakmile jsou soukromé informace odcizeny, je zde velké riziko jejich zneužití, ať už jde o odcizení finančních prostředků nebo využití identity ke spáchání trestného činu. Vymýšlejí se různé způsoby, jak získat soukromé informace, ale mezi ty nejčastější patří:
    - Podobný spoofing – je typ podvodu, při kterém kyberzločinci vytvoří přesnou kopii existující webové stránky. Většinou se jedná o e-shopy, kde uživatelé poskytují informace o své platební kartě, které jsou poté odcizeny. Tyto kopie jsou čím dál přesvědčivější a od původních webových stránek je čím dál obtížnější je rozeznat. Uživatelé musí pečlivě zkoumat adresu URL, která je jedinečná na internetu. Nicméně i tato ochrana je náchylná k zaměnění, kdy stačí vyměnit jedno písmeno za téměř identické.

- Tradiční phishing – představuje základ phishingových útoků, kde škodlivý e-mail simuluje běžný důvěryhodný e-mail. V e-mailu jsou vyžádané cenné informace oběti pomocí emocionálních podnětů.
- Invoice Phishing – je odesílán uživatelům na e-mail s tvrzením o nezaplacení zboží nebo služby, a s odkazem na zobrazení podrobnějších informací a následného uhrazení.
- Stahování – je dalším běžným způsobem phishingu. Jedná se o zaslání falešného e-mailu, ve kterém příjemce žádá o otevření nebo stažení dokumentu, obvykle s výzvou k přihlášení.
- Spear phishing – je extrémně cílený a vyžaduje intenzivní shromážděné veřejných, ale i soukromých informacích o životu oběti. E-mail je postaven na základě konkrétních prvků z života oběti.
- Ice phishing – se prosadil v důsledku vzestupu kryptoměn. Útočníci se vydávají za software peněženky nebo legitimní obchod, aby z účtu oběti odčerpali finanční prostředky. Odčerpání financí je dosaženo iniciací několika transakcí v různých obchodech.
- Smishing and Vishing – jsou phishingové útoky prováděné pomocí telefonních zpráv a hovorů. Smishingové útoky jsou postaveny na pocitu naléhavosti, kde jde o zavedení oběti na falešné vstupní stránky pro získání skutečných přihlašovacích údajů oběti. Příkladem Vishingu je situace, kdy se útočníci snaží vylákat SIM karty.
- Kompromitace firemních e-mailů – také známé jako Whaling, tyto e-maily mobilizují principy sociálního inženýrství. Útočníci se vydávají za autoritu v organizaci s vyšším postavením, než je oběť. Konečným cílem je změna oprávnění v interním systému. [14, 17]

- Ransomware – zašifruje soubory a adresáře, čímž se stávají nedostupnými pro všechny uživatele kromě útočníka. Ten uživatelům poskytne dešifrovací klíč pouze pokud zaplatí požadovanou částku ve formě kryptoměny nebo anonymní platební metody. Při nezaplacení částky hrozí běžnému uživateli ztráta dat, avšak organizaci hrozí poškození pověsti, výpadek provozu, právní a finanční postihy. Avšak i tak se nedoporučuje platit výkupné, jelikož není jisté, že útočník poskytne dešifrovací klíč. Lidský faktor

hraje při obraně ransomwaru velkou roli. Zaměstnanci v organizaci by měli být informování o prevenci napadení ransomwaru při školení. Ransomware vyvíjí chování malwaru, které se projevuje využíváním zranitelnosti a dalších cest útoku. Ransomware WannaCry využívá zranitelnosti v operačních systémech a (Not)Petya zneužívá chybu v programech. Ransomware se do operačního systému dostane přes e-mailové přílohy nebo nebezpečné webové stránky. Starší operační systémy jsou lehčí k napadení tímto způsobem. Data jsou zašifrována pomocí RSA nebo RC4. [14, 18]

5.2 Opatření proti kybernetickým hrozbám

Operační systém nabízí řadu opatření proti kybernetickým hrozbám:

- Secure Boot UEFI – kontroluje integritu zaváděcího procesu před načtením operačního systému. Pro načtení pouze důvěryhodného zavaděče operačního systému slouží modul TPM.
- Pravidelné aktualizace – zajišťují nejaktuálnější ochranu proti nejnovějším zranitelnostem. Tudíž jsou méně náchylné k útokům.
- Zálohování dat – je nezbytnou součástí posílení operačního systému pro zmírnění účinků hrozeb v rámci dat. Nedostupná data mohou být rychle obnovena záložní kopií dat i operačního systému v případě útoku. Doporučuje se uchovávat tři záložní kopie na dvou různých mediích a jedno z těchto medií uchovávat mimo pracoviště. Zálohy by se měly také pravidelně kontrolovat v rámci funkčnosti a integrity dat. [14, 15, 20]
- Exchange Online Protection – filtruje nevyžádanou poštu a pomáhá chránit e-maily, soubory a internetová úložiště před viry.
- Sledování síťového provozu prostřednictvím brány firewall – je zajištěné pomocí systému detekce a prevence. Systém detekuje neobvyklé aktivity a snaží se jim zabránit, ať už kontaktováním správce nebo zablokováním připojení podezřelé komunikace. Fungování systému je rozděleno do čtyř etap: sběr dat, výběr prvků, analýza a akce. [14, 19]
- Omezený přístup – umožňuje ověřeným uživatelům a legitimnímu provozu ochrání data a aplikace před zašifrováním. Silná hesla a vícefaktorové

ověřování poskytuje dodatečné zabezpečení, které zabrání neoprávněným uživatelům v přístupu. [14, 20]

- Vynucování bezpečného přístupu prostřednictvím minimálních oprávnění a omezení uživatelů.

5.3 Bezpečnostní metody

- Identifikace a autentizace – jsou vyžádané operačním systémem pro identifikaci totožnosti uživatele. Autentizace přiřazuje uživatelskou identitu k danému uživateli.
- Řízení přístupu – je klíčovým nástrojem pro zabezpečení operačního systému, který se skládá ze tří fází:
    - Autorizace
    - Povolení přístupu
    - Uložení povolení přístupu
- Nejmenší privilegia – znamenají, že uživatelům budou povolena oprávnění, která jsou potřebná k provedení jejich práce.
- Důvěryhodný kanál – zajišťuje ochranu dat, aby nešly převzít během přenosu přes aplikační vrstvu.
- Ochrana proti virům – v současné době se využívá antivirová ochrana, která je nezbytná k identifikaci a v rámci možností eliminaci kybernetických hrozeb. Dříve se viry a malware detekovaly pomocí jejich jedinečné signatury. Avšak dnes se uplatňuje spíše emulace kódu, heuristika a analýza chování k identifikaci různých hrozeb a jejich variant. Tyto hrozby jsou následně zaznamenány do virové databáze. Pro detekování a zamezení hrozeb vznikajících na zařízení koncového uživatele se začalo využívat strojového učení s využitím sandboxu a cloudové kontroly. Díky těmto pokročilým technologiím jsou antivirové programy schopny identifikovat i aplikace, které mohou negativně ovlivnit výkon operačního systému nebo zobrazovat nežádoucí obsah. [14, 21]

5.4 Objekt zásad skupiny

Pokud není uvedeno jinak, vychází text následující kapitoly ze zdrojů [22, 23].

Jedná se o soubor nastavení pravidel skupiny vytvořený firmou Microsoft pro definici, jak daný operační systém bude vypadat a jak se bude chovat pro určitou skupinu uživatelů. Objekty zásad skupiny jsou standartní součástí Active Directory a jsou spravovány jejím prostřednictvím. Zde jsou objekty zásad skupiny přiřazeny kontejnerům jako jsou weby, domény nebo organizační jednotky. Správci systému pomocí objektů zásad skupiny spravují aplikace, softwarové operace a uživatelské nastavení. Při použití konzole pro správu zásad skupiny mohou správci systému vytvořit objekt zásad skupiny, který definuje zásady založené na registrech, možnostech zabezpečení, instalaci a údržbě softwaru, skriptů i přesměrování složek.

5.4.1 Typy objektů zásad skupiny

Existují tři základní typy objektů zásad skupiny:

- Místní objekty zásad skupiny – se vztahují pouze na lokální počítače a uživatele, kteří se k tomuto počítači přihlašují. Místní objekty zásad skupin existují ve výchozím nastavení, ve všech počítačích s operačním systémem Windows. Používají se v případě, že nastavení skupinových zásad se má vztahovat na konkrétní počítač nebo jeho uživatele.
- Nemístné objekty zásad skupiny – jsou vázané na počítače nebo uživatele, jakmile jsou propojeny s objekty služby Active Directory. Nemístné objekty zásad skupiny jsou využity, pokud se nastavení zásad týká více počítačů nebo uživatelů.
- Startovací objekty zásad skupiny – jsou šablony pro nastavení skupinových zásad, které byly představené v operačním systému Windows Server 2008. Slouží jako předkonfigurovaný základ pro všechny budoucí zásady, které mají být vytvořeny.

5.4.2 Benefity použití objektů zásad skupiny

Hlavním benefitem aplikace objektů zásad skupiny je zvýšení zabezpečení uživatelských počítačů v rámci celé organizace před vnitřními hrozbami i vnějšími útočníky. Objekty zásad skupiny v rámci zabezpečení mohou zbránit uživatelům přístup k citlivým informacím nebo k provádění úloh, které by mohly ohrozit kritické systémy nebo data. Avšak využití objektů zásad skupin nese řadu dalších výhod, mezi které patří:

- Efektivní správa – je dosažena díky již zavedeným objektům zásad skupiny. Tyto zavedené objekty zásad skupiny aplikují standardizované prostředí pro všechny nové uživatele a počítače, kteří se připojí k doméně organizace. Tímto způsobem se šetří čas potřebný k nastavení.
- Snadná správa – vzniká pomocí objektů zásad skupiny, přes které lze nasazovat software, záplaty a další aktualizace z jednoho místa, a rozhraní služby Active Directory.
- Lepší prosazování zásad hesel – spočívá v nastavení objektů zásad skupiny vlastností hesel, jako je délka hesel, opakované použití konkrétních hesel, složitost hesel a pravidelné vypršení platnosti pro zabezpečení sítě společnosti.
- Lepší ochrana složek – je umožněna objektem zásad skupiny, který zajistí, aby uživatelé uchovávali důležité firemní soubory v centralizovaném a monitorovaném úložném systému. Přesměrování složek na síťové úložiště chrání soubory v místních počítačích.

5.4.3 Limity objektů zásad skupiny

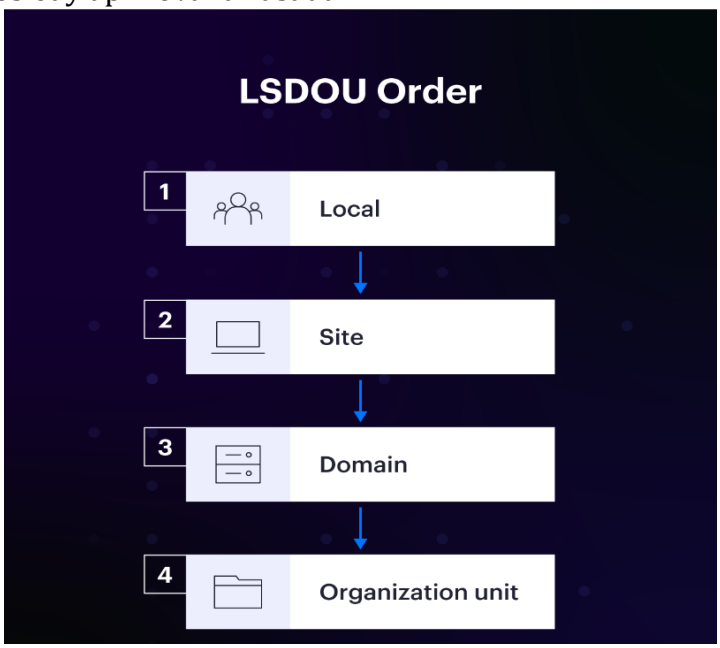
Při využití objektů zásad skupiny se lze potkat i s různými omezeními:

- Probíhají postupně – s tím, že i jejich akce se zpracovávají jedna po druhé. To při velkém zavedení objektů zásad skupiny může vést k delšímu přihlášení uživatele.
- Flexibilita je omezená – a vztažená přímo na počítače a uživatele. Omezenost vzniká, když se jedná o použití nastavení na základě kontextu.

- Omezené spouštěče – vyvolávají aplikaci objektů zásad skupiny. Mezi takové spouštěče patří spuštění počítače, přihlášení uživatele nebo přednastavené intervaly. Objekty zásad skupiny nemohou reagovat na změny prostředí. Třeba jako je odpojení a opětovné připojení k síti.
- Obtížná údržba – vzniká při vyhledávání nebo filtrování pro nalezení konkrétního nastavení v rámci objektu zásad skupiny, což stěžuje vyhledávání nebo opravu problémů s existujícím nastavením.
- Žádná kontrola verzí – znamená, že provedené změny v nastavení objektu zásad skupiny nejsou kontrolovány. Při nesprávné změně nelze jednoduše zjistit, o jakou konkrétní změnu se jednalo a kdo ji provedl.

5.4.4 Pořadí zpracování objektů zásad skupiny

Obrázek 7 zobrazuje pořadí zpracování objektů zásad skupiny. Nejprve se zpracují skupinové zásady v lokálním počítači. Za nimi následují skupinové zásady kontejnerů Active Directory od úrovně webu až po doménu. A jako poslední se zpracují organizační jednotky. Objekty zásad skupiny, které jsou vnořené v rámci organizačních jednotek, se provádí od nejbližší organizační jednotky, až po kořenovou jednotku a odtud odcházejí. Při jakémkoliv konfliktu má přednost a účinnost naposledy aplikovaná zásada.



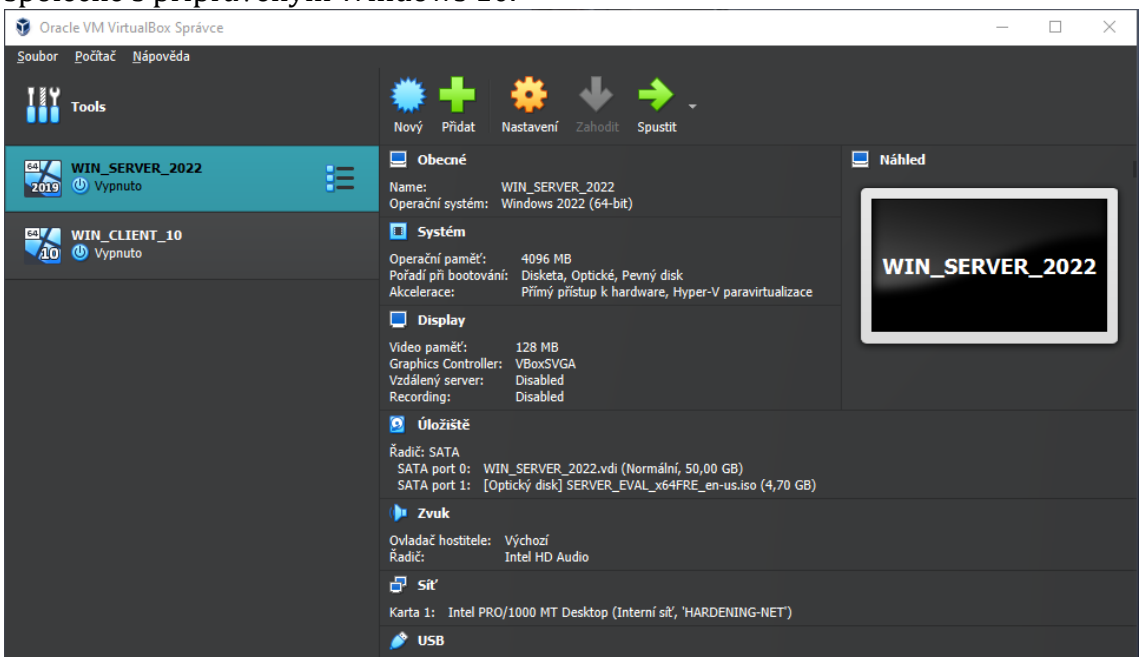
Obrázek 7 – LSDOU pořadí zpracování objektů skupinových zásad. Zdroj [22]

6 Praktické řešení – Hardening

V praktické části se bakalářská práce věnuje představení Hardeningu v reálné praxi. Pro simulaci reálné praxe je představena firma, která vyvíjí weby na míru. Daná firma se skládá z několika programátorů, vedoucího programátora, designerů, vedoucího designera, konzultantů, projektových manažerů, hlavního manažera firmy, ředitele firmy a správce serveru. Následující praktická část bude simulována v programu VirtualBox, který lze nalézt a stáhnout z https://www.virtualbox.org/wiki/Downloads.

6.1 Příprava virtuálního prostředí

Po úspěšné instalaci VirtualBoxu lze připravit virtuální prostředí pro Windows Server 2022 a Windows 10. Obrázek 8 zobrazuje konkrétní nastavení specifikací Windows Serveru 2022 po dokončení přidání virtuálního prostředí společně s připraveným Windows 10.

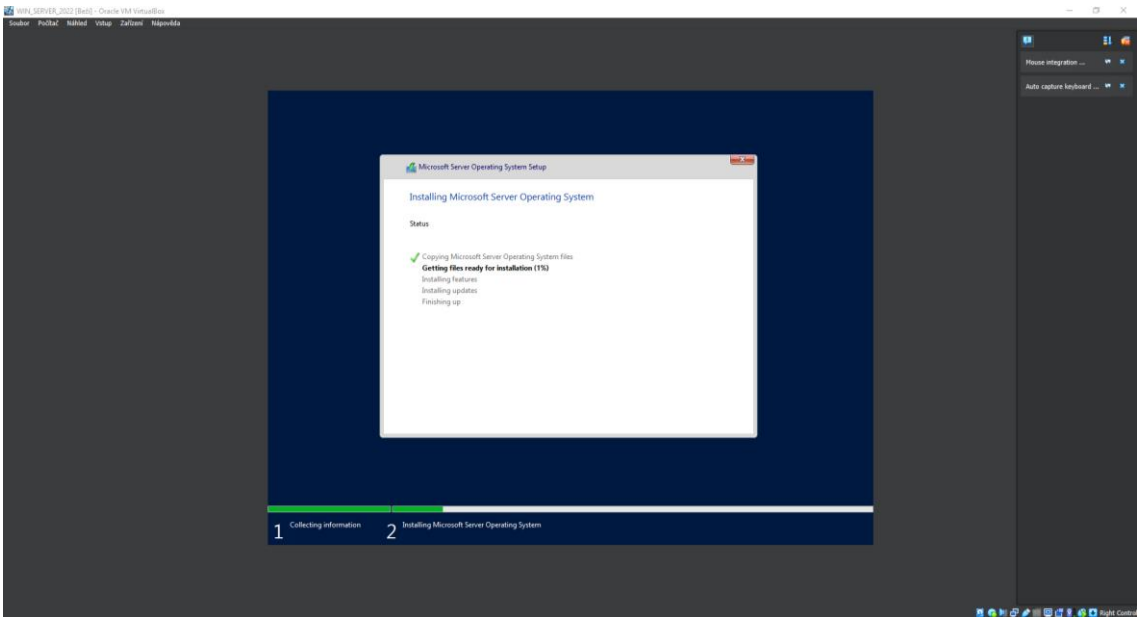


Obrázek 8 – VirtualBox – Příprava virtuálního prostředí. Zdroj: vlastní

6.2 Instalace Windows Serveru

Instalace Windows Serveru 2022 probíhá stejně jako každá jiná instalace operačního systému Windows. V případě možnosti jazyka operačního systému si uživatel může vybrat preferovaný jazyk. Následně klikne na tlačítko Instalovat

a bude přesunut na výběr edicí, kde si může zvolit konkrétní edici a zda daná edice má obsahovat plné grafické rozhraní či nikoliv. Potvrzení licenčních podmínek je základem jakéhokoliv softwaru. Posledním uživatelským nastavením je výběr úložiště, kde bude daný Windows Server 2022 nainstalován. Obrázek 9 ukazuje klasické instalování operačního systému Windows, které může několik minut trvat.



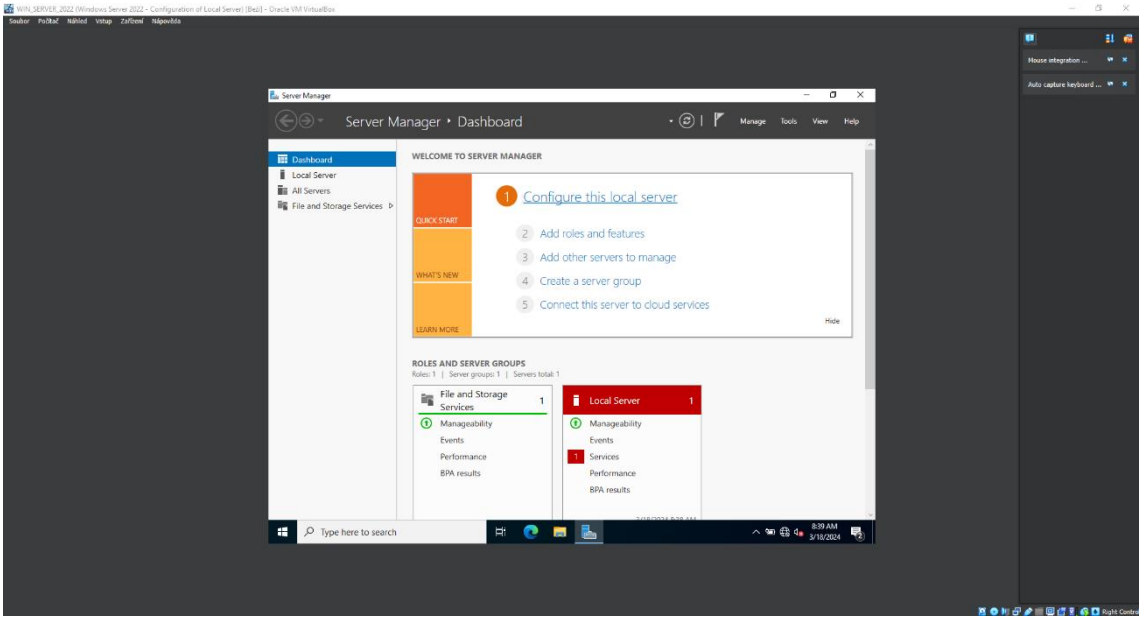
Obrázek 9 – Windows Server – Instalace OS. Zdroj: vlastní

Po dokončení instalace Windows Serveru 2022 se zařízení restartuje a přenese uživatele na nastavení hesla pro lokálního administrátora. Když se uživatel přihlásí jako administrátor otevře se mu automaticky aplikace Server Manager, ve které se později bude konfigurovat Windows Server. Avšak nejdříve pro lepší plynulost VirtualBoxu se doporučuje nainstalovat přídavky pro hosta a nechat Windows Server restartovat pro zavedení těchto přídavků.

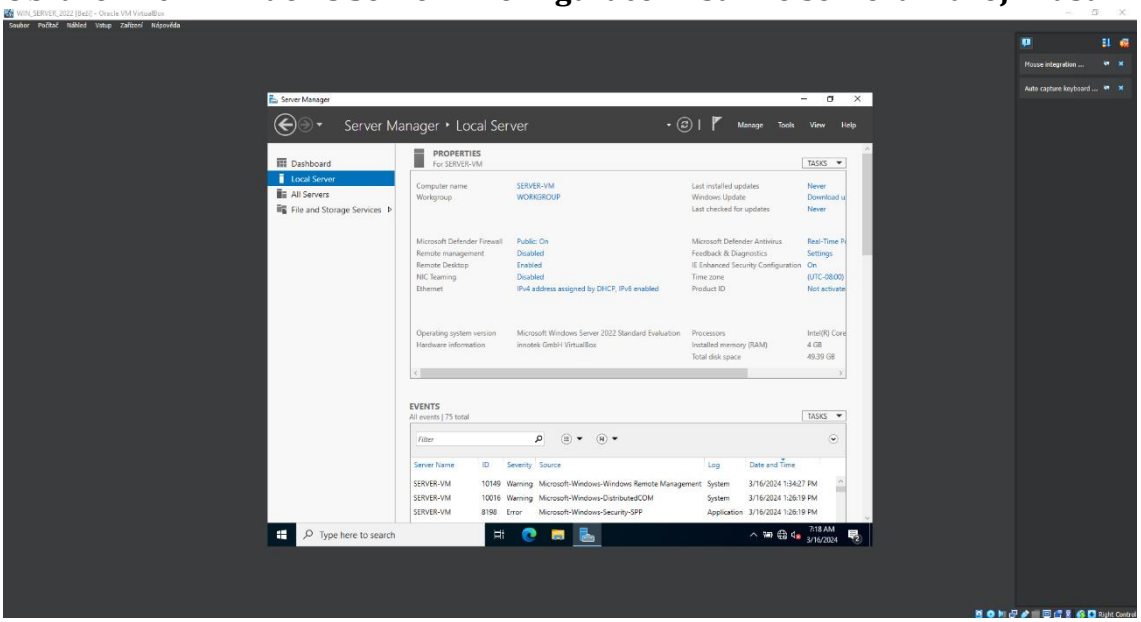
6.3 Konfigurace Windows Serveru

Jak již bylo řečeno konfigurace Windows Server bude probíhat v aplikaci Správce serveru, kde pro započetí uživatel klikne na možnost Konfigurovat tento místní server. Tato možnost ho přesměruje na položku Local Server a zde lze vidět vlastnosti daného Windows Serveru. Před počátkem konfigurace Windows Serveru je dobré mu změnit název na něco generického. Po restartování Windows Serveru je vhodné zakázat Vzdálenou správu a povolit Vzdálenou plochu s přidáním výjimky do Firewallu. Obrázek 10 a Obrázek 11 zobrazují hlavní panel Správce serveru

s možností konfigurace místního serveru a položku Local Server, kde jsou zřetelné vlastnosti Windows Serveru 2022.



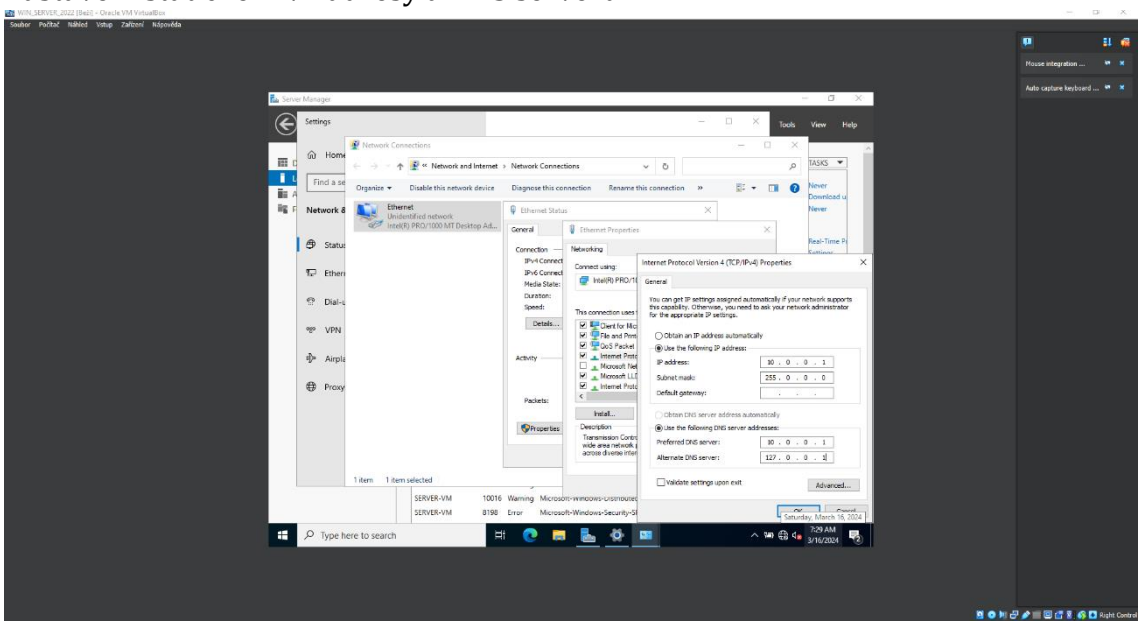
Obrázek 10 – Windows Server – Konfigurace místního serveru. Zdroj: vlastní



Obrázek 11 – Windows server – Vlastnosti lokálního serveru. Zdroj: vlastní

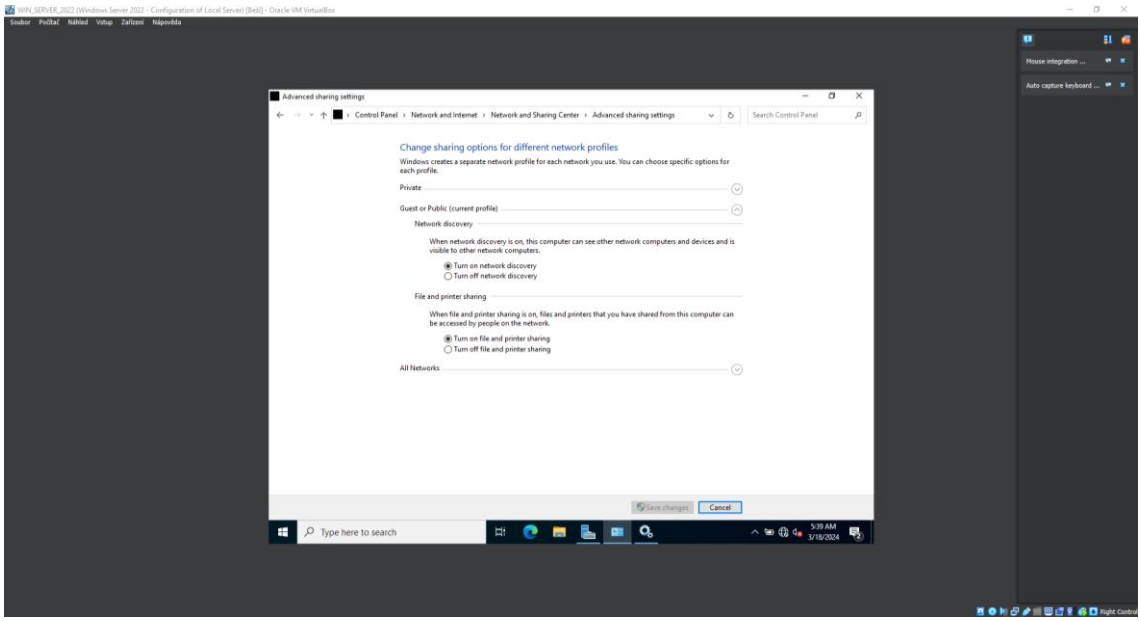
Dalším krokem pro konfiguraci Windows Serveru bude nastavit statickou IPv4 adresu. Je několik cest, jak se dostat do síťového nastavení, zde byla využita cesta: Hlavní panel (ikona síťového připojení) -> Otevřít nastavení Síť a internet -> Změnit možnosti adaptéru. Pro otevření okna Ethernet – stav je potřeba dvakrát kliknout na daný adaptér. V tomto okně se klikne na tlačítko Vlastnosti a následně na možnost Protokol IP verze 4 (TCP/IPv4). Ve vlastnostech pro protokol IP verze 4 (TCP/IPv4) uživatel musí zadat statickou IP adresu a vyplnit Upřednostňovaný

server DNS a stejně tak i Alternativní server DNS. Obrázek 12 zobrazuje konkrétní nastavení statické IPv4 adresy a DNS serverů.



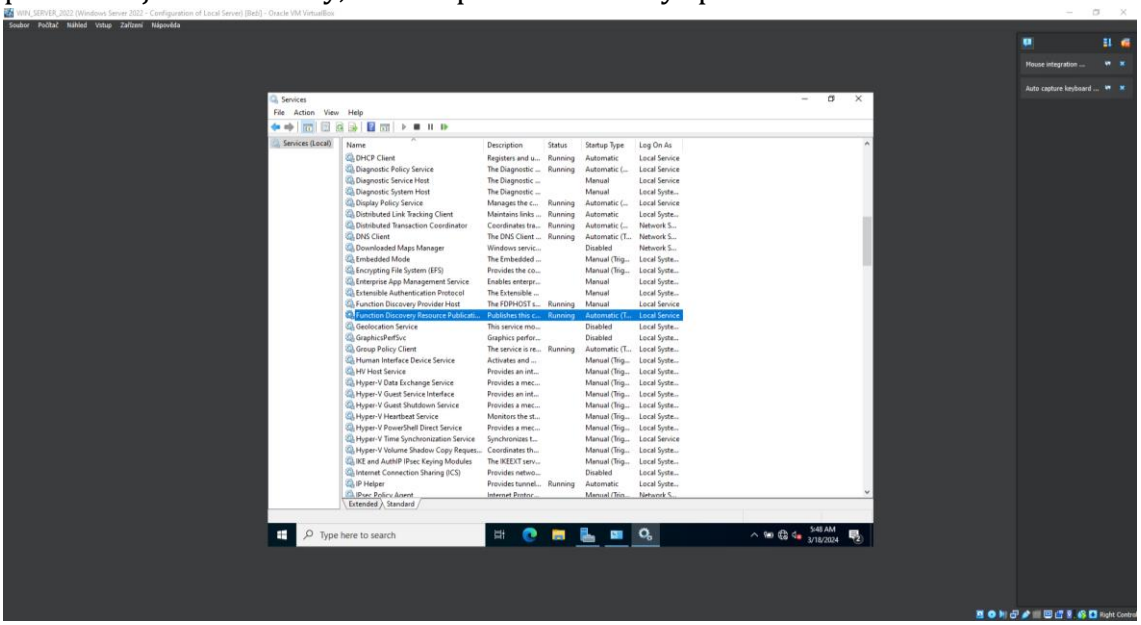
Obrázek 12 – Windows Server – Nastavení statické IPv4 adresy. Zdroj: vlastní

Aby Windows Server zůstal v síti viditelný, je potřeba změnit pokročilé nastavení sdílení. Toho lze dosáhnout otevřením Ovládacích panelů -> Síť a internet -> Centrum síťových připojení a sdílení, a v levé části okna kliknout na možnost Změnit pokročilé nastavení sdílení. Zde uživatel musí zapnout možnosti zjišťování sítě a sdílení souborů a tiskáren v podkategoriích Host nebo veřejný. Obrázek 13 zobrazuje zapnutí pokročilých nastavení sdílení.



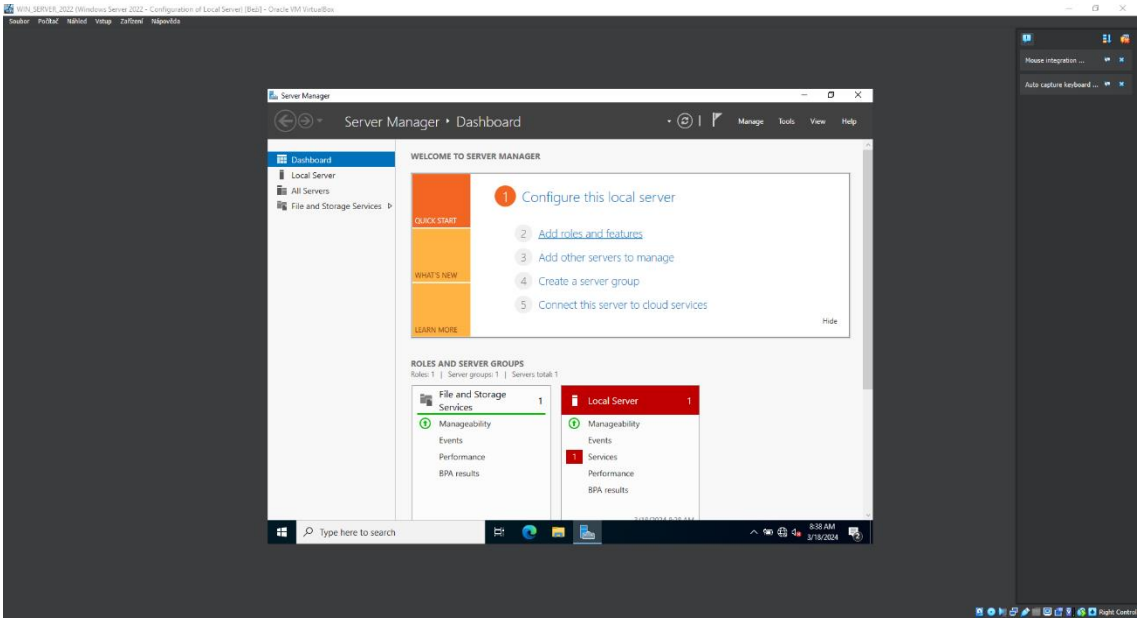
Obrázek 13 – Windows Server – Pokročilé nastavení sdílení. Zdroj: vlastní

Může se stát, že možnost zjišťování sítě nezůstane permanentně zapnutá. Pro takový případ je potřeba ověřit, zda běží potřebné služby: Klient DNS, Publikování prostředků rozpoznání funkcí, Objevování SSDP a Hostitel zařízení UPnP. K ověření těchto služeb je potřeba otevřít aplikaci Služby. Ta se jednoduše otevře pomocí klávesové zkratky Windows+R a do okna Spustit se napíše services.msc. Zde už jednoduše stačí dohledat potřebné služby a spustit je. Pokud některá ze služeb nepůjde spustit, tak je potřeba nejprve spustit ostatní služby a k této se vrátit až jako poslední. Pro eliminaci potřeby ručního spuštění při každém zapnutí Windows Serveru je dobré nastavit automatické spuštění. Obrázek 14 představuje okno Služby, kde lze potřebné služby spustit.

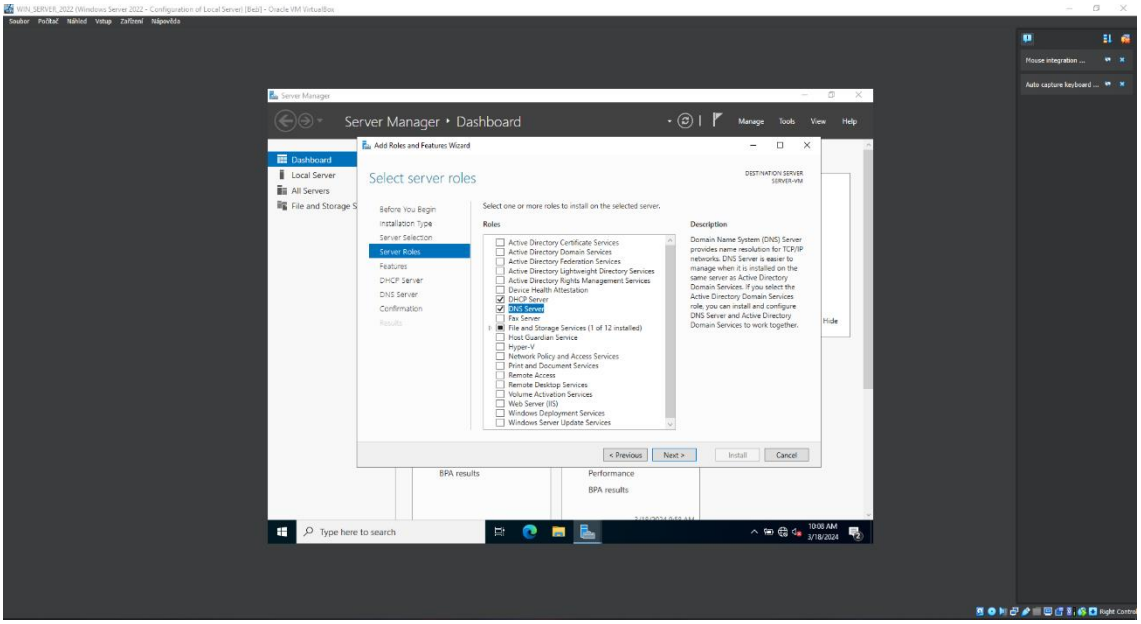


Obrázek 14 – Windows Server – Spuštění služeb zjištění sítě. Zdroj: vlastní

Mezi hlavní část konfigurace Windows Serveru patří instalace rolí DNS a DHCP. Pro instalaci těchto rolí uživatel klikne na možnost Přidat role a funkce na hlavním panelu Správce serveru. Obrázek 15 zobrazuje hlavní panel Správce serveru s možností Přidání rolí a funkcí. Otevře se průvodce přidání rolí a funkcí. V Průvodci přidání rolí a funkcí do části Role serveru se nemusí nic měnit. V Typu instalace je potřeba se ujistit, že je zaškrtnutá možnost Instalace na základě rolí nebo funkcí a při Výběru server bude zobrazen název daného Windows Serveru. V časti Role serveru uživatel zaškrtne Server DHCP a Server DNS. Při zvolení těchto možnost se objeví okno s přidáním potřebných funkcí pro Server DHCP a Server DNS, které se musí potvrdit. Obrázek 16 ilustruje hotový výběr Rolí serveru.



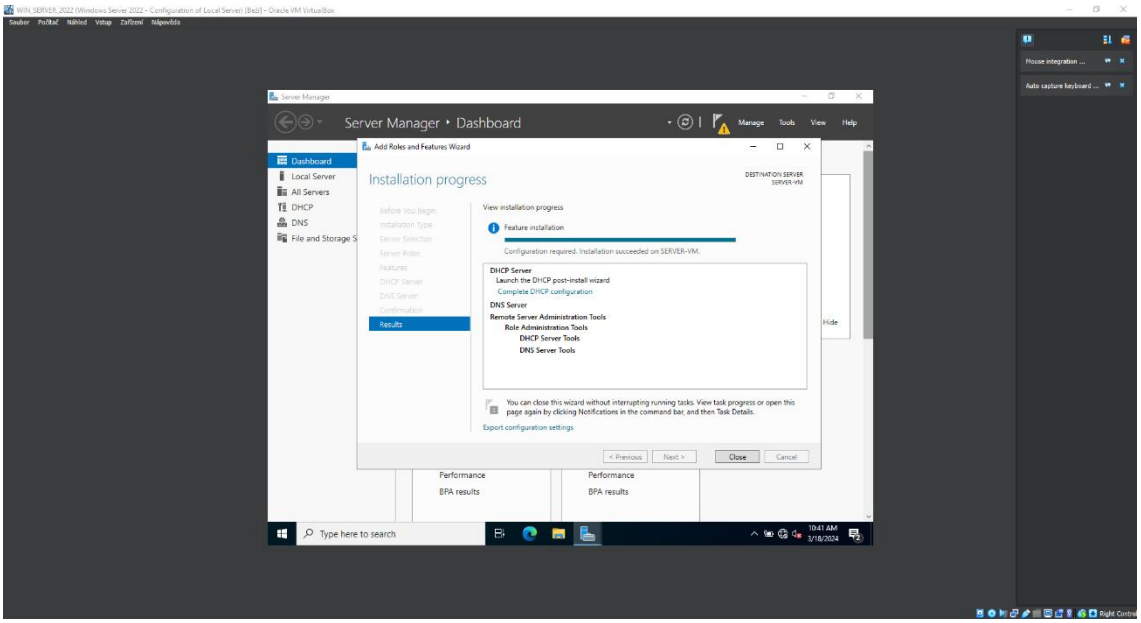
Obrázek 15 – Windows Server – Přidání rolí a funkcí. Zdroj: vlastní



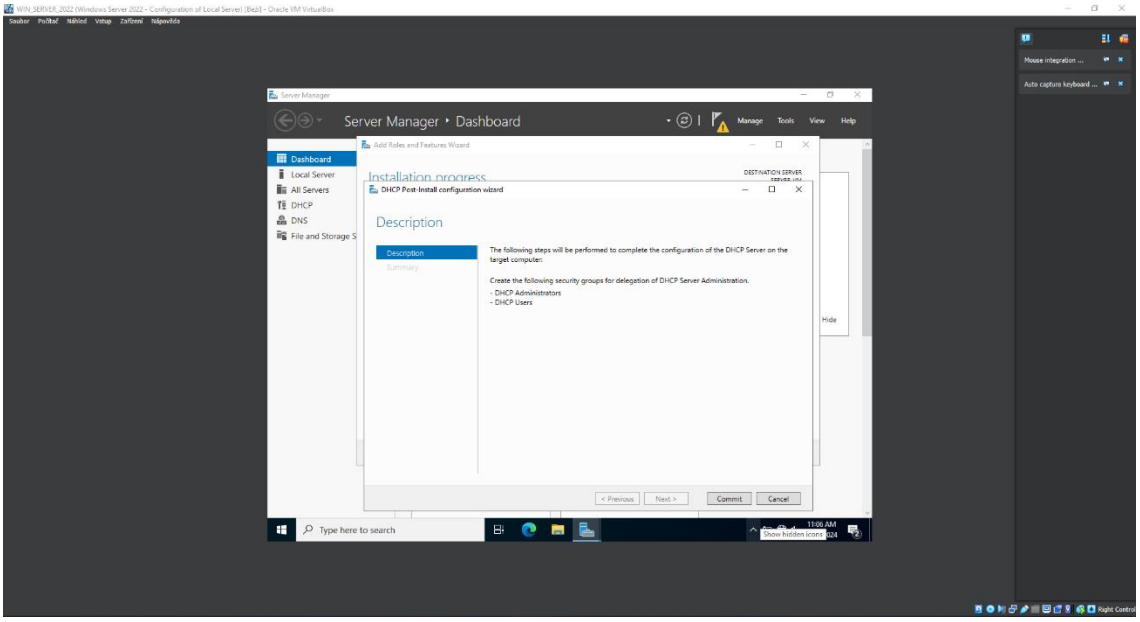
Obrázek 16 – Windows Server – Výběr DHCP a DNS Serveru. Zdroj: vlastní

Dále lze beze změn proklikat průvodce až na konec a tlačítkem Nainstalovat se zahájí instalace serverových rolí. Výsledky úspěšné instalace jsou zobrazeny formou výpisu instalace a přidaných funkcí. V daném výpisu lze vidět, že je potřeba dokončit konfiguraci DHCP Serveru. Obrázek 17 shrnuje výsledek instalace serverových rolí. Pro dokončení postinstalační konfigurace je nutné kliknout na možnost Dokončit konfiguraci služby DHCP. Uživatel bude následně přesměrován na průvodce postinstalační konfigurace DHCP. Zde se jedná pouze o vytvoření skupin DHCP Administrators a DHCP Users. Obrázek 18 odkazuje

na průvodce postinstalační konfigurace DHCP a přidání potřebných skupin DHCP pro dokončení konfigurace.



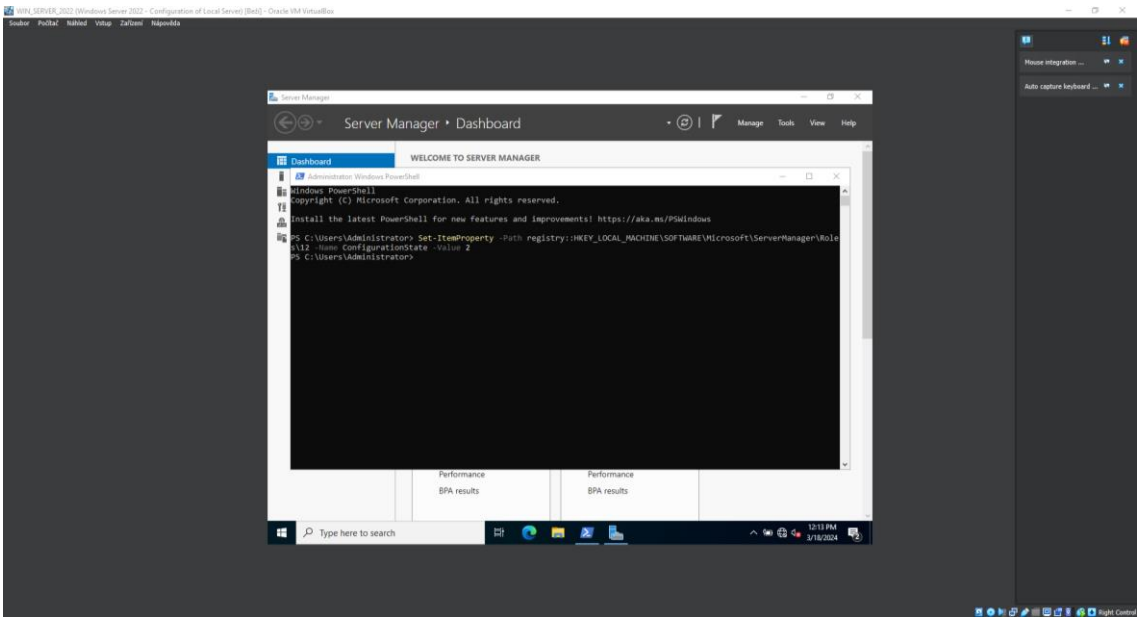
Obrázek 17 – Windows Server – Hotová instalace server rolí. Zdroj: vlastní



Obrázek 18 – Windows Server – Dokončení konfigurace DHCP. Zdroj: vlastní

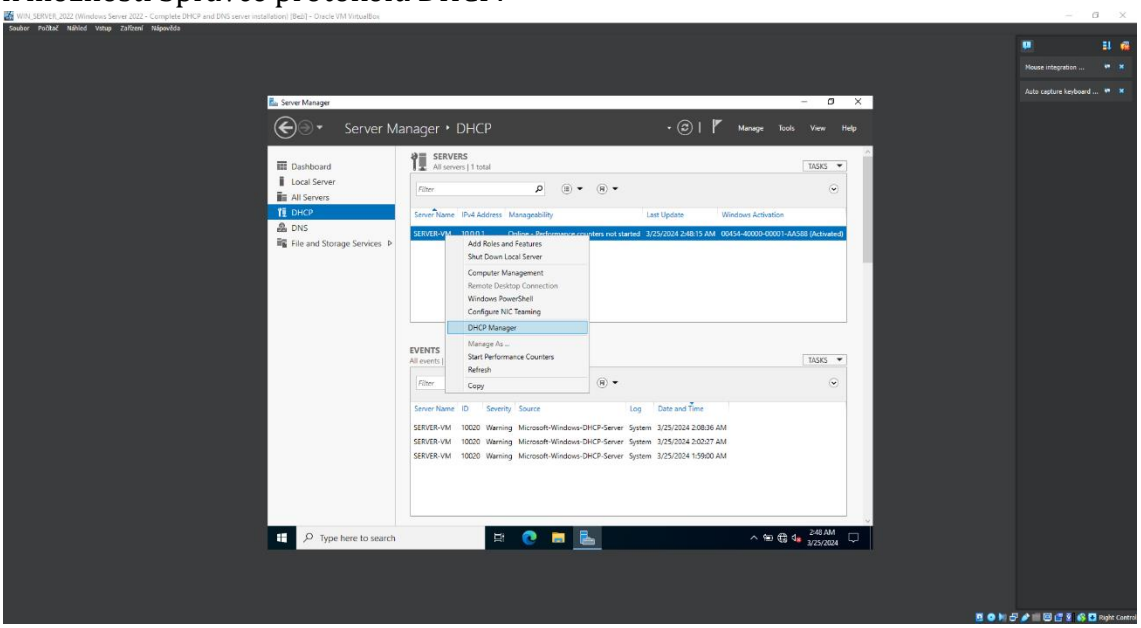
V rámci obvyklého zpracování by stačilo kliknout na tlačítko potvrdit a je hotovo, ovšem může se objevit tykající nezdaření otevření klíče registru v cílovém počítači pro nastavení postkonfigurační úlohy. V takovém případě je potřeba otevřít aplikaci Windows PowerShell jako správce a napsat příkaz: Set-ItemProperty –Path registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager\Roles\12 –Name ConfigurationState –Value 2. Následně stačí vypnout a znovu spustit

Správce serveru a konfigurace DHCP Serveru je kompletní. Obrázek 19 vizualizuje příkaz v Powershellu.



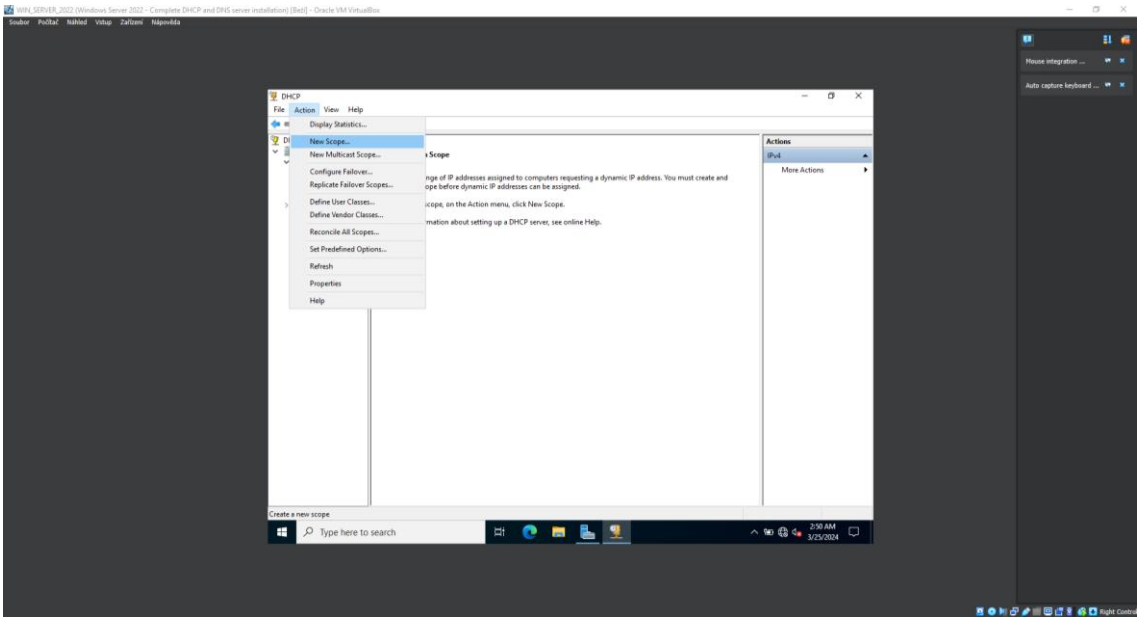
Obrázek 19 – Windows Server – PowerShell – dokončení DHCP. Zdroj: vlastní

Po dokončení konfigurace DHCP Serveru v rámci Správce serveru zbývá nastavit DHCP pro správné fungování. Ve Správci serveru lze vidět na bočním panelu, že se vlevo zobrazují položky DHCP a DNS. Uživatel klikne na DHCP, označí název serveru a pravým tlačítkem si rozbalí kontextové menu, kde ho zajímá Správce protokolu DHCP. Obrázek 20 zobrazuje cestu daného postupu, jak se dostat k možnosti Správce protokolu DHCP.



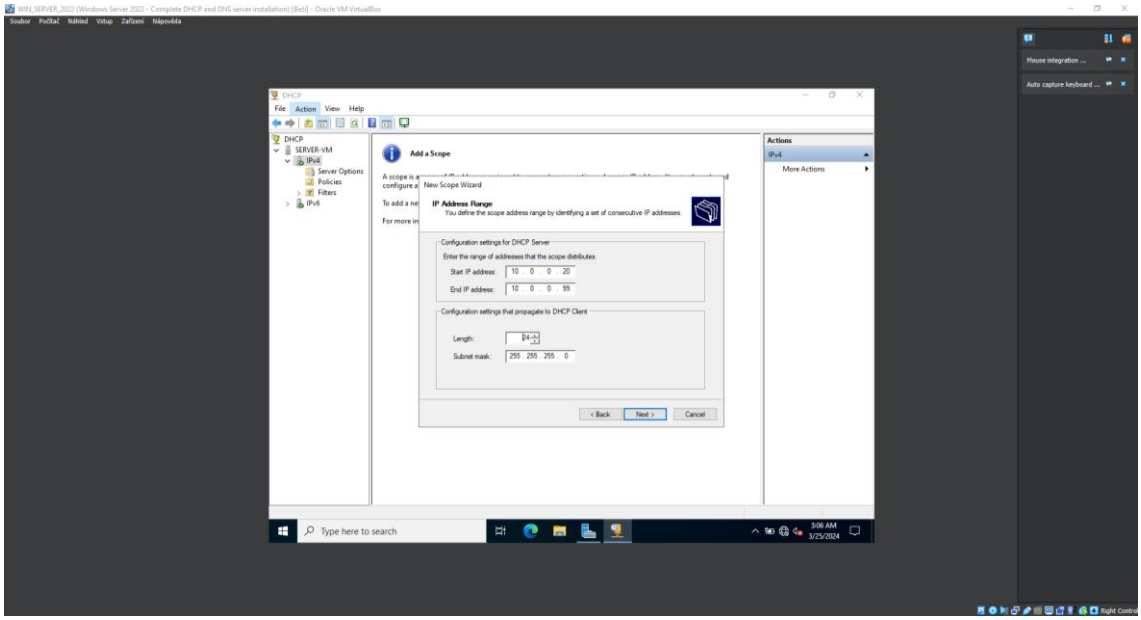
Obrázek 20 – Windows Server – Správce protokolu DHCP. Zdroj: vlastní

Ve správci protokolu DHCP v bočním levém panelu uživatel rozbalí položku s názvem daného serveru a následně označí možnost IPv4. Nahoře otevře kartu Akce a vybereme možnost Nový obor, což mu otevře průvodce pro vytvoření nového oboru DHCP. Obrázek 21 ukazuje, kde se vytváří nový obor.



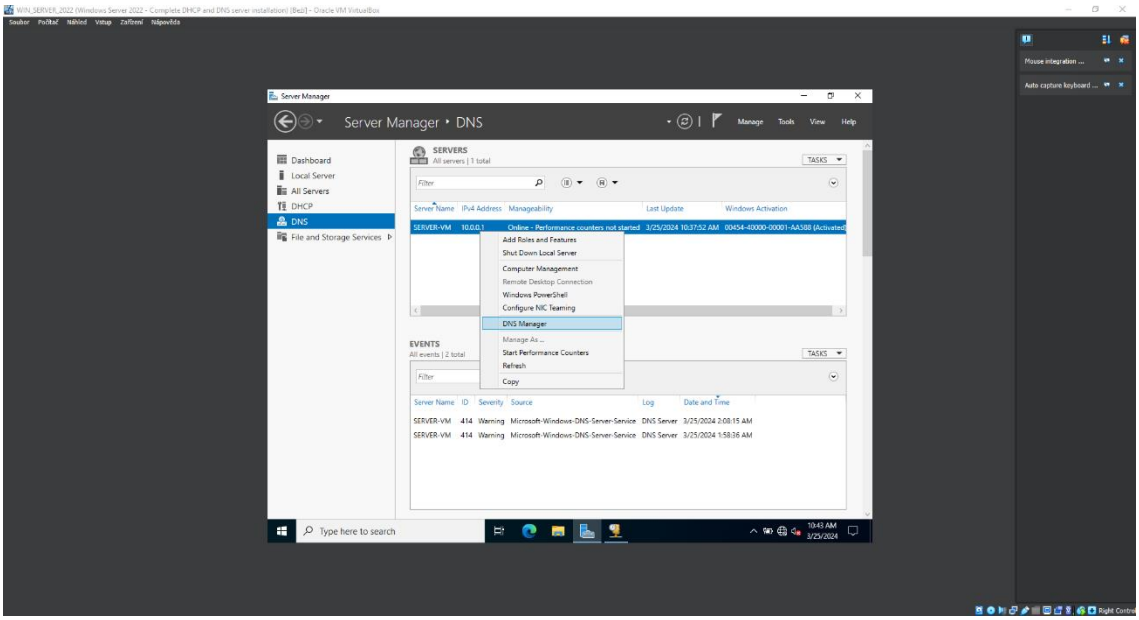
Obrázek 21 – Windows Server – DHCP – Nový obor. Zdroj: vlastní

V průvodci v prvním okně zadá libovolné jméno oboru. Ve druhém okně nastaví rozsah IP adres, které budou poskytovány zařízením v síti. Obrázek 22 představuje rozsah použitých IP adres v tomto případě. Na dalším okně Přidání vyloučení a zpoždění se nemusí nic zadávat, pouze v případě, pokud by bylo požadováno nastavení vyloučení některé z IP adresu v daném rozsahu. Na následujícím okně lze upravit dobu zapůjčení IP adresy. V tomto případě doba zapůjčení byla nastavena na 1 den. Další okno se ptá uživatele, zda si přeje nakonfigurovat možnosti služby DHCP pro vytvořený obor, kde zvolí možnost Ano, chci nakonfigurovat tyto možnosti teď. Do dalšího okna musí přidat IP adresu směrovače neboli IP adresu daného Windows Serveru. V posledním okně Název domény a servery DNS se přidá nadřazená doména simulované firmy a zkontroluje se, že klientská zařízení budou používat DNS servery pomocí IP adresy Windows Serveru. Pak už lze se proklikat na konec průvodce a aktivovat obor.



Obrázek 22 – Windows Server – DHCP – Rozsah IP adres. Zdroj: vlastní

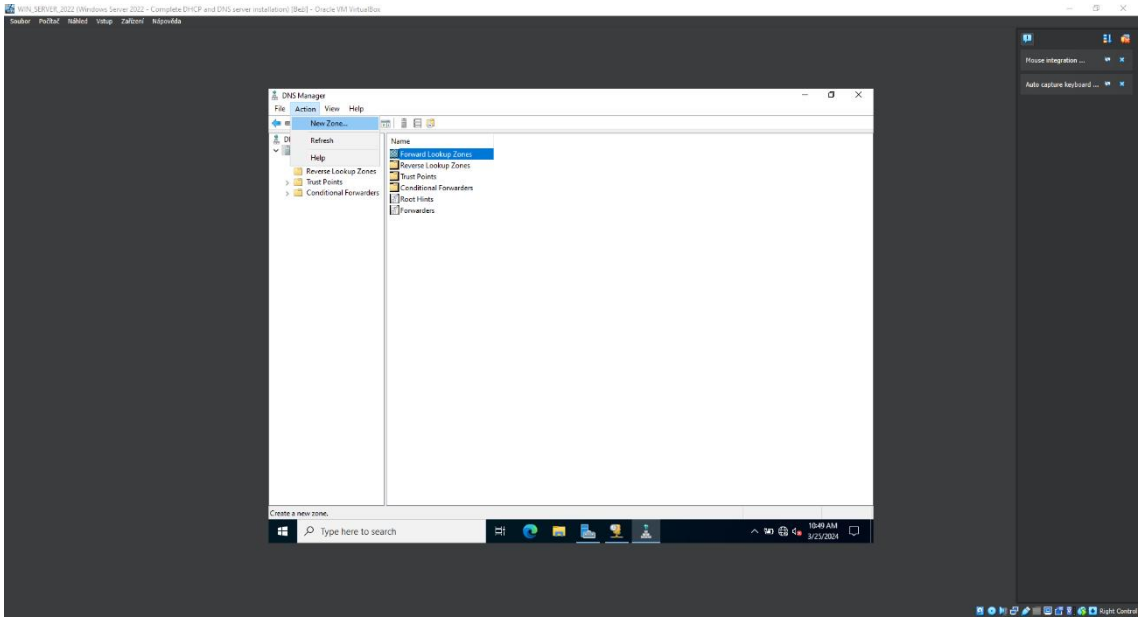
Nový obor nemusí stoprocentně fungovat, protože ještě zbývá nakonfigurovat službu DNS. Pro správné nastavení služby DNS je potřeba se dostat do aplikace Správce DNS. Postup otevření Správce DNS je stejný jako u Správce protokolu DHCP, jenom s tím rozdílem, že se v bočním panelu zvolí možnost DNS. Obrázek 23 znázorňuje cestu k aplikaci Správce DNS.



Obrázek 23 – Windows Server – Správce DNS. Zdroj: vlastní

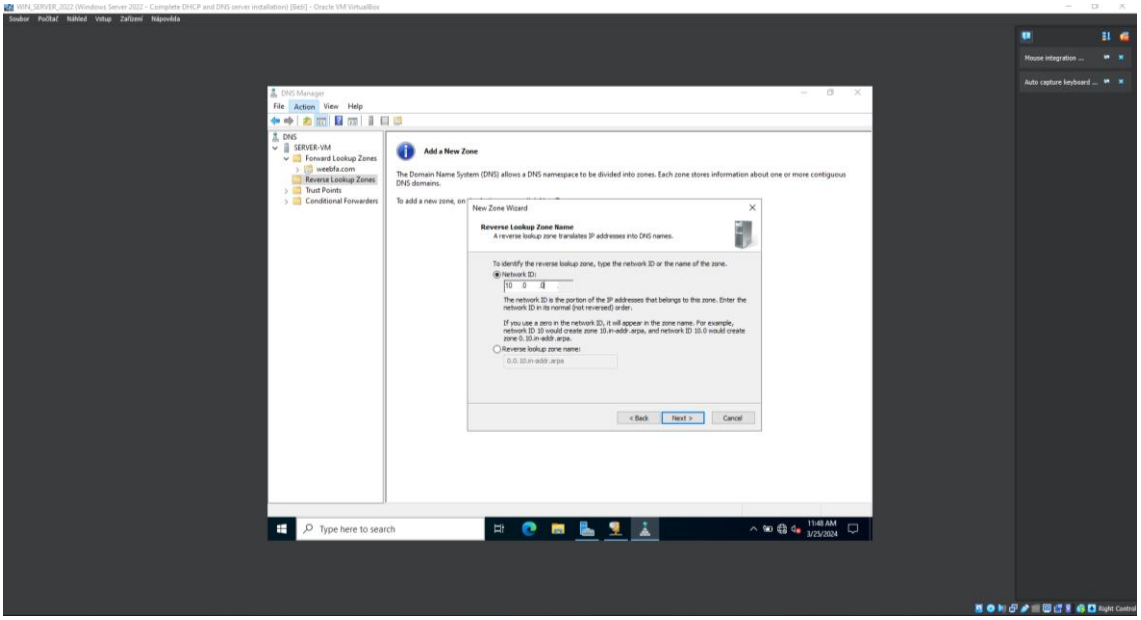
Ve Správci DNS v levém bočním panelu uživatel označí daný Windows Server pro zobrazení zón dopředného a zpětného vyhledávání. Pro správné fungování DNS služby je potřeba nastavit obě zóny vyhledávání. Avšak nejdříve je zřejmé začít s vytvořením zóny pro dopředné vyhledávání. Uživatel si označí Zóny dopředného

dohledávání a v horním panelu zvolí nabídku Akce a Nová zóna. Tím se otevře průvodce pro vytvoření nové zóny. Obrázek 24 prezentuje Správce DNS a vytvoření nové dopředné zóny.



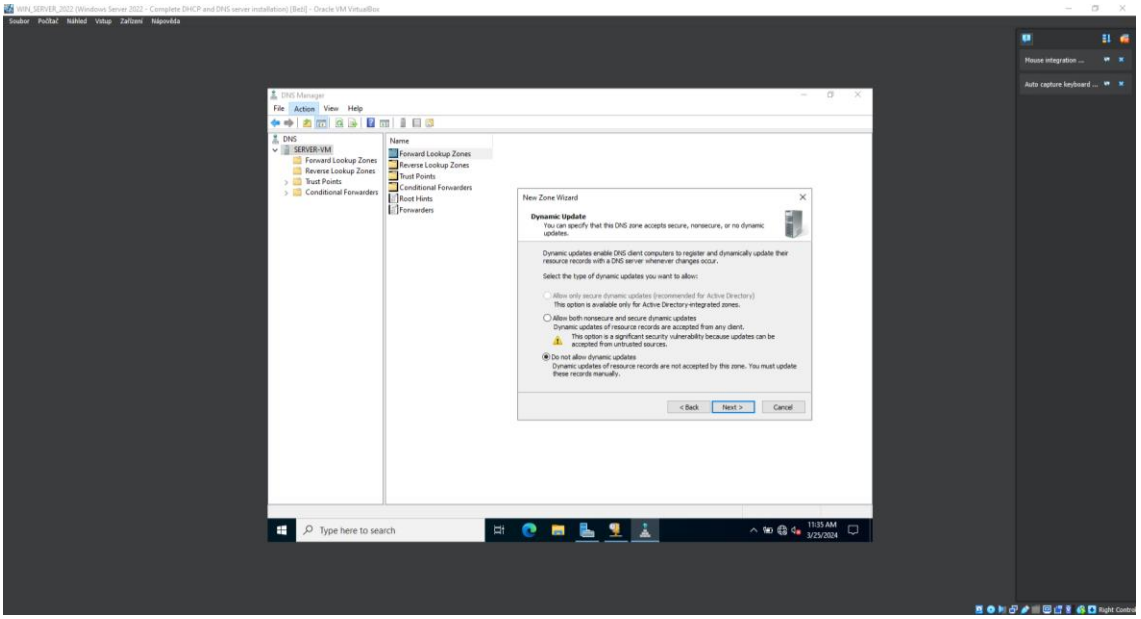
Obrázek 24 – Windows Server – DNS – Nová dopředná zóna. Zdroj: vlastní

První stránku lze přeskočit tlačítkem Další. Na druhé stránce uživatel zvolí možnost Primární zóna a pojmenuji ji stejně jako název nadřazené domény, který uváděl při nastavení protokolu DHCP. Na další stránce si nechá vytvořit soubor, jehož název se skládá z jména dané domény a koncovky .dns. Následující karta vykazuje první prvky zabezpečení neboli hardeningu. Jedná se o povolení dynamických aktualizací s možnostmi: Povolit pouze zabezpečené dynamické aktualizace, Povolit zabezpečené i nezabezpečené dynamické aktualizace a Nepovolit dynamické aktualizace. V případě nainstalované Active Directory bych se zvolila první možnost, nicméně v této fázi Active Directory ještě nebylo nainstalováno, takže prozatím se nechá možnost Nepovolit dynamické aktualizace. Obrázek 25 ilustruje rozhodnutí o dynamický aktualizací DNS záznamů. Ke konci stačí dojít průvodce Vytvoření nové zóny a podobným způsobem vytvořit i zónu pro zpětné vyhledávání.



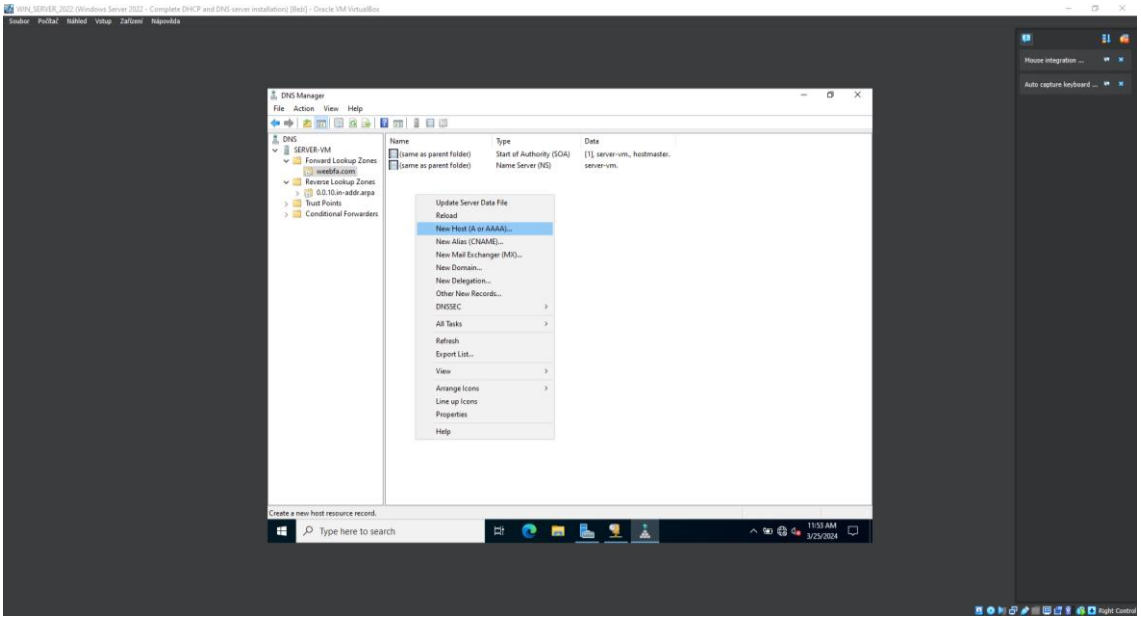
Obrázek 25 – Windows Server – DNS – Dynamické aktualizace. Zdroj: vlastní

Vytvoření nové zóny pro zpětné vyhledávání je odlišné pouze ve zvolení konkrétní nové zóny v rámci adresy IPv4 a přidání ID sítě. Obrázek 26 znázorňuje přidání ID sítě v rámci tvoření nové zóny zpětného vyhledávání.



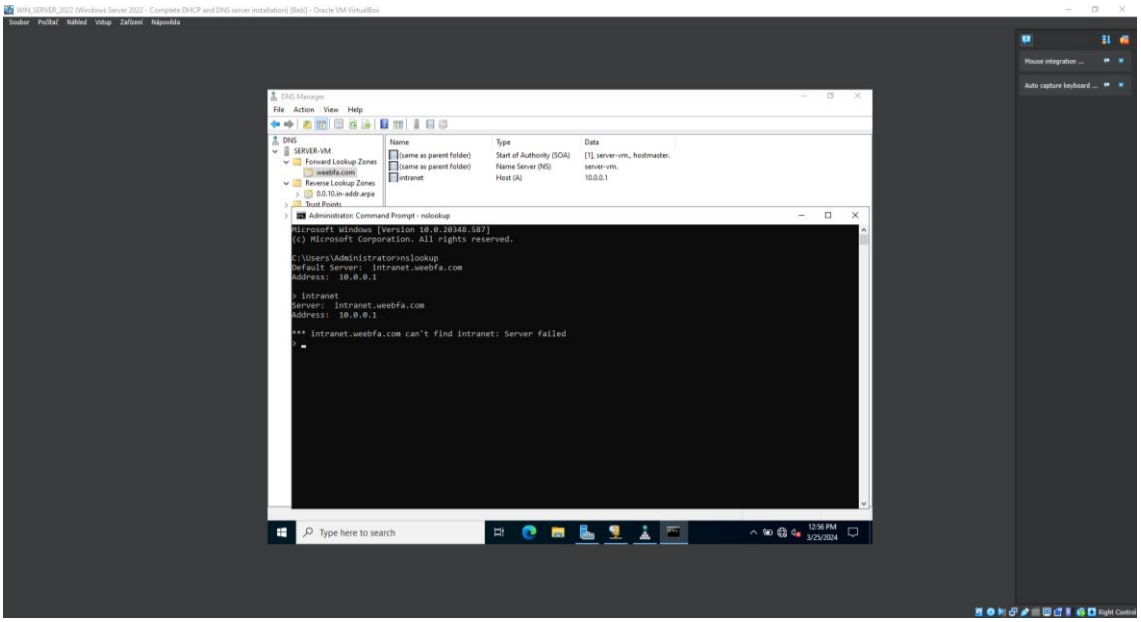
Obrázek 26 – Windows Server – DNS – ID Sítě. Zdroj: vlastní

Když jsou DNS zóny vytvořené, je potřeba vytvořit DNS záznam, který bude odkazovat na Windows Server ve formě intranetu. Záznam lze vytvořit označením položky Zóny dopředného vyhledávání a zde otevřít kontextové menu a v něm možnost Nový hostitel (A nebo AAAA). Obrázek 27 ukazuje způsob vytvoření nového DNS záznamu.



Obrázek 27 – Windows Server – Vytvoření DNS záznamu. Zdroj: vlastní

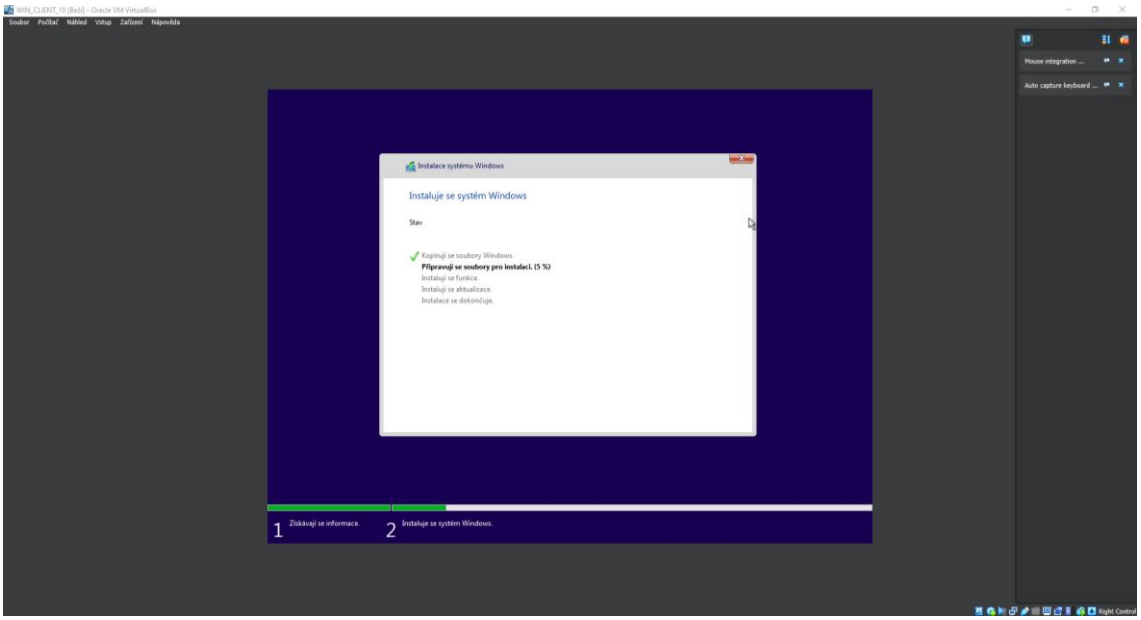
Díky tomu se otevře okno s názvem nový hostitel, ve kterém lze zadat název v podobě intranet a IPv4 adresu Windows Serveru. Poslední věcí je zaškrtnutí políčka Vytvořit přidružený záznam o ukazateli (PTR). Ověření funkčnosti služby DNS lze ověřit v příkazové řádce příkazem nslookup jako Administrátor. Tento příkaz vypíše předklad vytvořené domény na IP adresu a IP adresu na doménový název. Obrázek 28 představuje výpis příkazové řádky po zaznamenání příkazu nslookup. První odpověď naznačuje funkční DNS službu. Ovšem druhá odpověď vykazuje chybovou hlášku, která je zaměřena na chybějící část Active Directory.



Obrázek 28 – Windows Server – Ověření funkčnosti DNS. Zdroj: vlastní

6.4 Instalace Windows klienta

Instalace klasického Windows 10 klienta je ještě o něco jednoduší než instalace Windows Serveru 2022. Při spuštění připraveného virtuálního prostředí se jako první zobrazí výběr nastavení jazyka a rozlišení klávesnice. Po stisknutí tlačítka Další a následně tlačítka Nainstalovat bude spuštěn průvodce k instalaci Windows 10 klienta. Jako při jakékoliv instalaci operačního systém Windows je žádán Product Key, avšak pro simulační účely lze zadat možnost Nemám kód Product Key. Mimo simulaci je důležité mít vždy platnou aktivaci operačního systému Windows. Po Product Key následuje vybrání edice operačního systému Windows. Verze Pro, jak už název napovídá, je profesionální edici, která má více funkcí než běžná edice Home. Takže pro lepší podmínky simulace se zvolí právě tato edice. Odsouhlasení licenčních podmínek a zvolení možnosti Vlastní v rámci typu instalace uživatele posune k možnostem operování s pamětí na disku. Pokud zde nejsou nějaké speciální požadavky na rozdělení disku na více oddílů, lze pokračovat dále. Na dalším okně bude probíhat instalační proces jako u Windows Serveru 2022. Obrázek 29 vizualizuje instalační proces Windows 10 klienta.



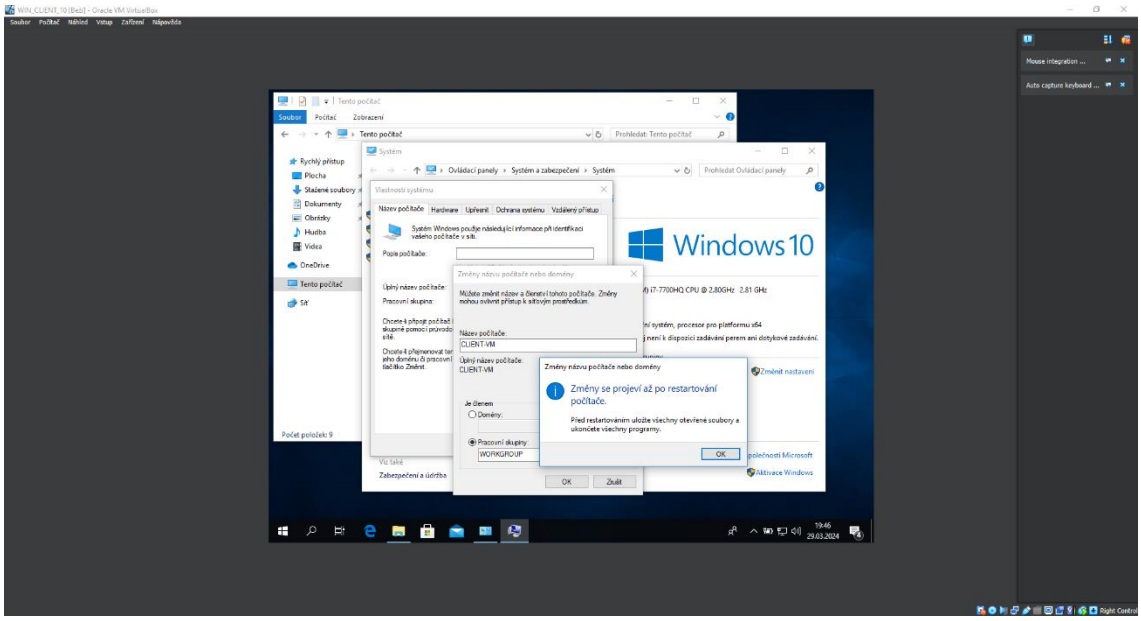
Obrázek 29 – Windows Klient – Instalace OS. Zdroj: vlastní

Po několika restartování a hotové instalaci je uživatel přenesen do více uživatelského přívětivějšího průvodce, který ho provede nastavením uživatelských preferencí. Mezi tyto preferenci patří opět nastavení jazyka a rozlišení klávesnice, aktuální stav operačního systému Windows 10 Pro, přihlašovací účet a služby.

Přihlašovací účet může být záludná záležitost. Dnes je doporučené se přihlašovat přes oficiální Microsoft účet, avšak v rámci této simulace byl vytvořen takzvaně Offline účet, který byl využit pro přihlášení do Windows 10 klienta, tento účet po nastavení Active Directory již nebude potřeba. Co se týče služeb, zde je lepší všechny služby potlačit nebo využít jenom základní verzi. Tyto služby od Microsoftu jsou spíše dodatkové a nejsou potřeba k fungování operačního systému Windows. Tudíž by se dalo o nich prohlásit, že se jedná o bloatware. Když si tím dlouhým procesem uživatel projede měl by skončit na domovské obrazovce operačního systému Microsoft Windows 10 Pro. Poslední krokem instalace přídavků pro hosta.

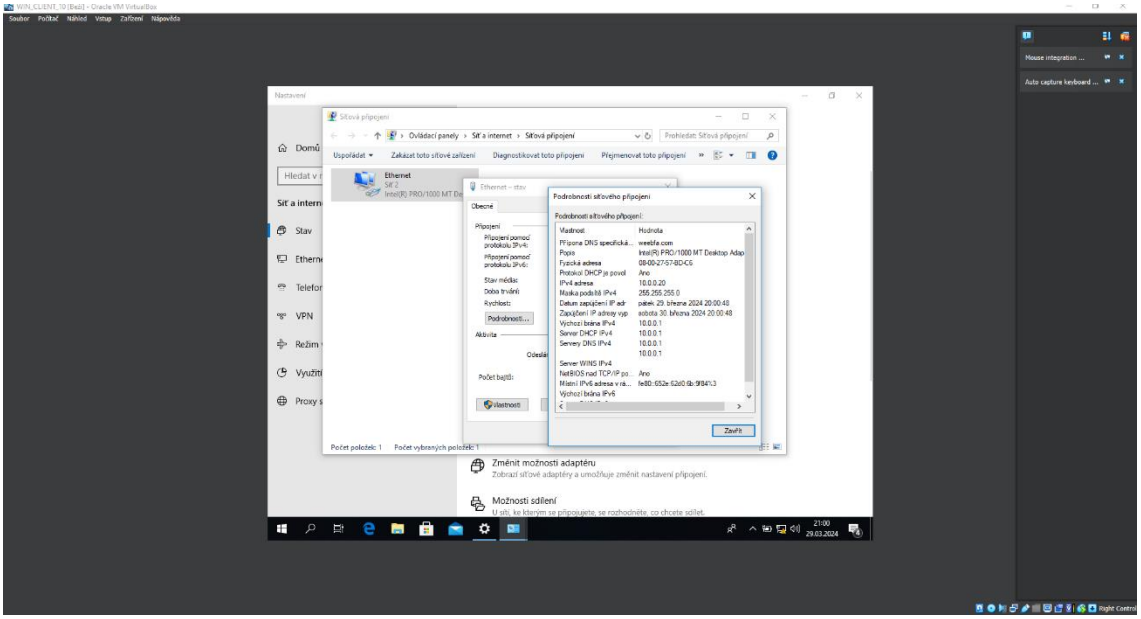
6.5 Konfigurace Windows klienta

Pro konfiguraci Windows 10 klienta není třeba dělat tolik kroků jako u Windows Serveru 2022. Avšak i zde je vhodnější změnit název na něco jednoduššího. Nejprve si uživatel otevře Průzkumníka souborů a v levém panelu si otevřeme kontextové menu položky Tento počítač. Tím se otevřou Základní informace o počítači. Vedle položky Název počítače se klikne na Změnit nastavení. Zobrazí se okno s Vlastnostmi systému a zde se klikne na tlačítko Změnit. V této sekci lze změnit název počítače. Následně na to je uživatel musí restartovat daný počítač pro uplatnění změny názvu počítače. Obrázek 30 představuje způsob cesty pro změnu názvu počítače ve Windows 10.



Obrázek 30 – Windows Klient – Změna názvu. Zdroj: vlastní

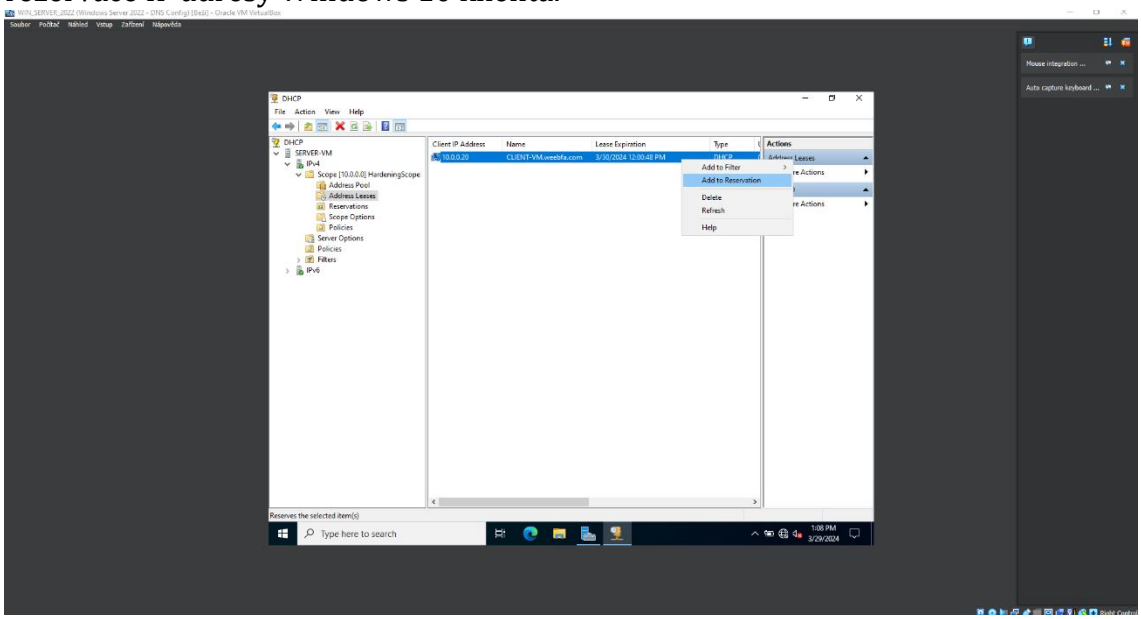
Dalším nastavením bude přepnout síť ve VirtualBoxu pro Windows 10 klienta. V horní liště je potřeba najít možnost Zařízení, pak Síť a otevře se okno Nastavení s položkou Síť. Tady stačí změnit možnost Připojena k: na Vnitřní síť a VirtualBox by měl automaticky doplnit stejný název sítě jako u Windows Serveru 2022. Jako poslední věcí je potřeba zajistit, aby Windows klient zůstal v síti viditelný. Toho lze dosáhnout stejným postupem jako u Windows Serveru. Stačí otevřít Ovládací panely -> Síť a internet -> Centrum síťových připojení a sdílení, a v levé části okna kliknout na možnost Změnit pokročilé nastavení sdílení. Aby připojení fungovalo bylo stabilní, stačí v kategorii Privátní zapnout možnost zjišťování sítě a sdílení souborů a tiskáren. Avšak pro budoucí účely je potřeba tyto možnosti zapnout i v kategorii Host nebo veřejný stejně jako u Windows Serveru. V tuto chvíli Windows 10 klient by měl obdržet IP adresu od DHCP serveru. To lze ověřit otevřením kontextové nabídky ikony připojení v levé části Hlavního panelu a možnost Otevřít nastavení Síť a internet. V otevřeném nastavení kliknout na možnost Změnit možnosti adaptéru, zde na daný Ethernet adaptér. V okně Ethernet – stav kliknout na tlačítko Podrobnosti. Obrázek 31 ukazuje okno s podrobnostmi síťového připojení.



Obrázek 31 – Windows Klient – IP adresa. Zdroj: vlastní

V tomto bodě by se dalo říct, že vše je nastavené, ovšem lze nastavit ještě jednu věc a tím je rezervace aktuální IP adresy pro Windows 10 klienta. Z výrazů již vyplývá, že rezervace spočívá v uchování aktuálně přidělené IP adresy pro daného

klienta při každém připojení. Pro rezervaci je potřeba na Windows Serveru 2022 otevřít Správce protokolu DHCP. Ten lze otevřít přes Správce serveru a v levé části okna položka DHCP. Následně označit název daného Windows Serveru pro otevření kontextové nabídky a zde vybrat Správce protokolu DHCP. Když se uživateli otevře okno Správce Protokolu, tak si v něm otevře jeho vytvořený obor a označí položku Zapůjčení adresy. Zde vybere daného Windows 10 klienta, otevře kontextové menu a klikne na možnost Přidat do rezervace. Obrázek 32 znázorňuje cestu a způsob rezervace IP adresy Windows 10 klienta.

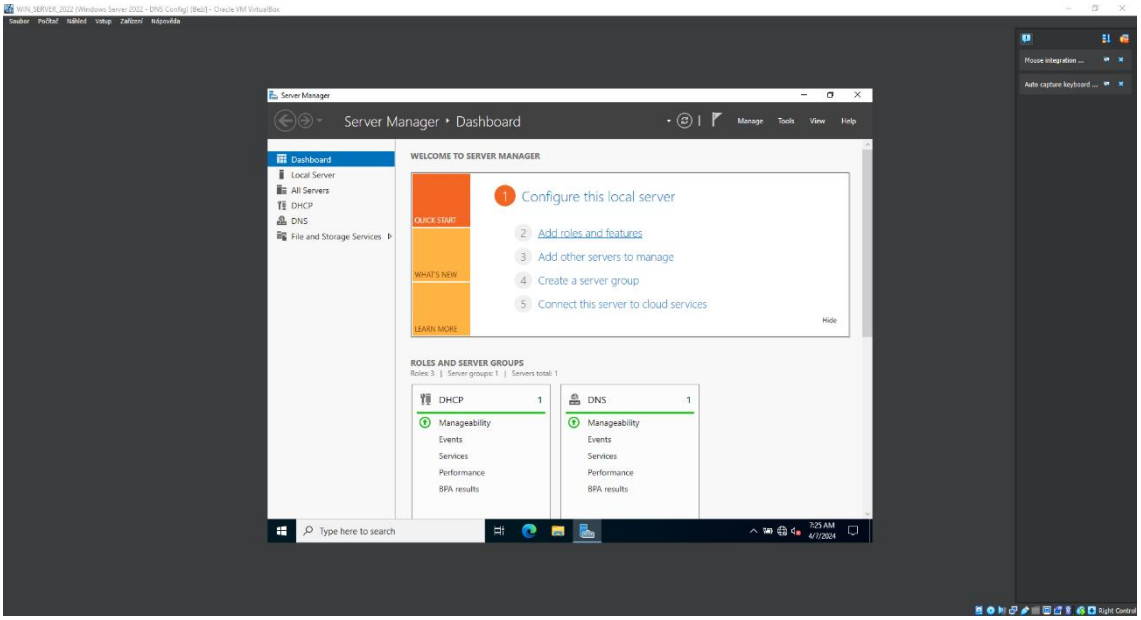


Obrázek 32 – Windows Server – DHCP – Rezervace IP adresy. Zdroj: vlastní

Teď měla být viditelná IP adresa Windows 10 klienta v položce Rezervace. Po rezervaci je možné ověřit ve Windows 10 klientu, zda DNS služba je funkční. Stejně jako u Windows Serveru 2022 stačí otevřít příkazový řádek a napsat příkaz nslookup. Pokud výstup příkazu nslookup je podobný tomu, co byl na Windows Serveru 2022, tak DNS služba je správně nakonfigurována a běží v pořádku.

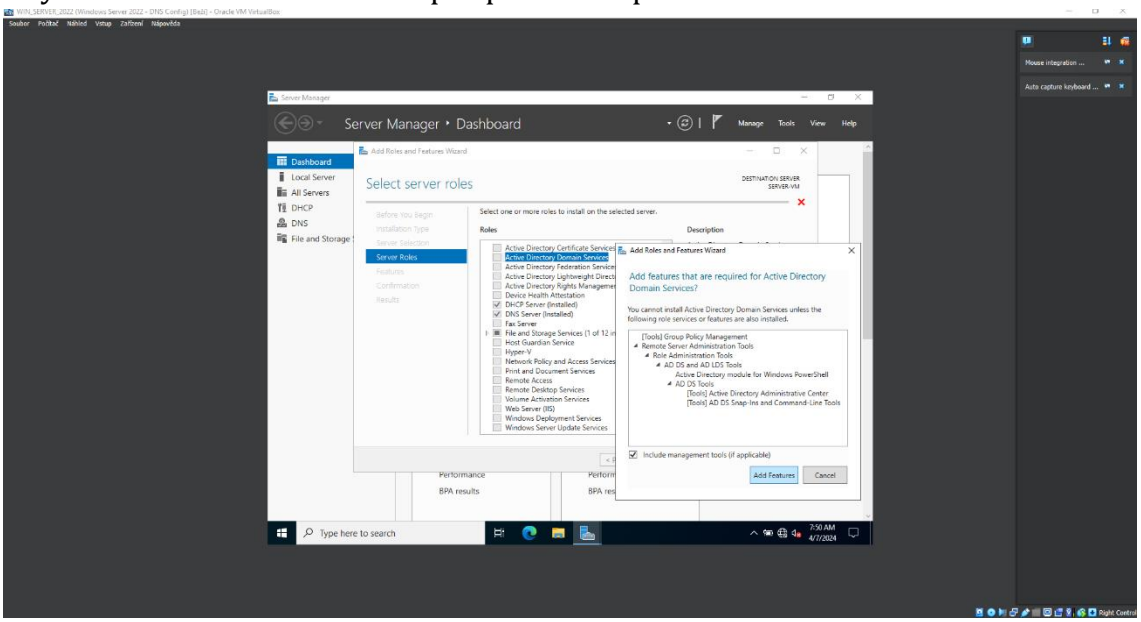
6.6 Active Directory

Důležitou součástí simulace hardeningu je nasazení a nastavení Active Directory, která slouží pro veškerou správu prvků v doméně. Ovšem prvním krokem je přidat službu Active Directory Domain Services ve Windows Serveru 2022. Stejně jako DHCP a DNS se tato služba přidává přes aplikaci Správce serveru a možnost Přidat role a funkce. Obrázek 33 znázorňuje možnost Přidat role a funkce ve Správci Serveru, avšak nyní lze vidět rozšířené možnosti v levém bočním panelu.



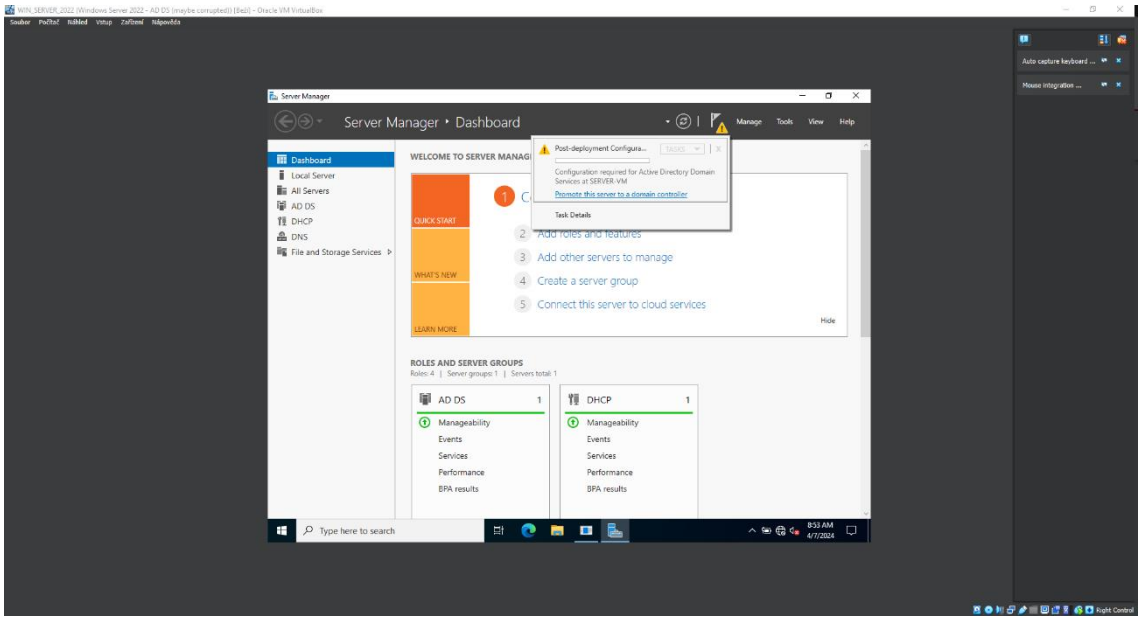
Obrázek 33 – Windows Server – Další přidání rolí a funkcí. Zdroj: vlastní

Když uživatel klikne na možnost Přidat role a funkce, otevře se mu opět stejný průvodce přidáním rolí a funkcí. V prvním okně jsou vysvětlené možnosti přidání rolí a funkcí, které lze jednoduše přeskočit tlačítkem Další. Ve druhém okně se ponechá vybraná výchozí možnost instalace na základě rolí nebo funkcí a v následujícím okně se ujistí, že se jedná o správný Windows Server. Ve výběrovém okně serverových rolí se zaškrtne možnost Active Directory Domain Services a ve vyskakovacím okně stačí kliknout na tlačítko Přidat funkci. Obrázek 34 ukazuje přidání služby Active Directory Domain Services ve výběru rolí nebo funkcí a vyskakovací okno s tlačítkem pro provedení přidání funkce.



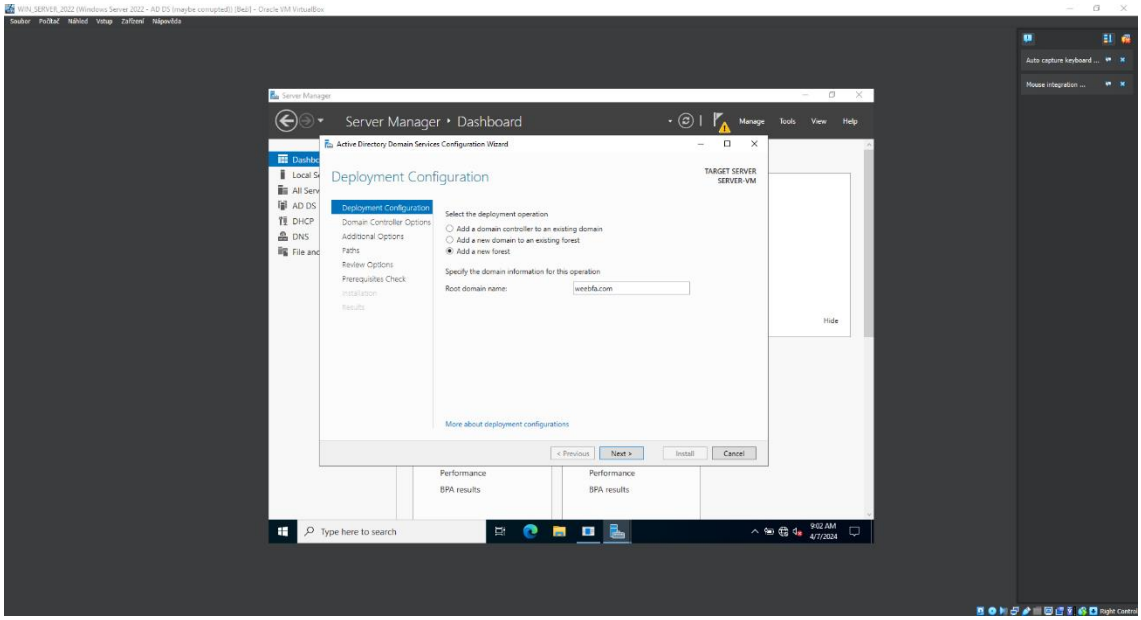
Obrázek 34 – Windows Server – Vybrání AD DS. Zdroj: vlastní

Následně je dostačující se proklikat průvodcem přidání rolí a funkcí pomocí tlačítka Další až k samotné instalaci služby Active Directory Domain Services. Po dokončené instalaci služby Active Directory Domain Services je potřeba povýšit Windows Server na řadič domény. Na tuto skutečnost Správce serveru upozorňuje stejně jako u konfigurace DHCP. V horní části Správce serveru lze spatřit ikonu oznámení, která nyní ukazuje symbol upozornění. V oznámení si lze povšimnout zprávy Konfigurace po nasazení a možnosti Povýšit tento server na řadič domény ve formě hypertextové odkazu. Obrázek 35 představuje nové upozornění s potřebou povýšit server na řadič domény.



Obrázek 35 – Windows Server – Server na řadič domény. Zdroj: vlastní

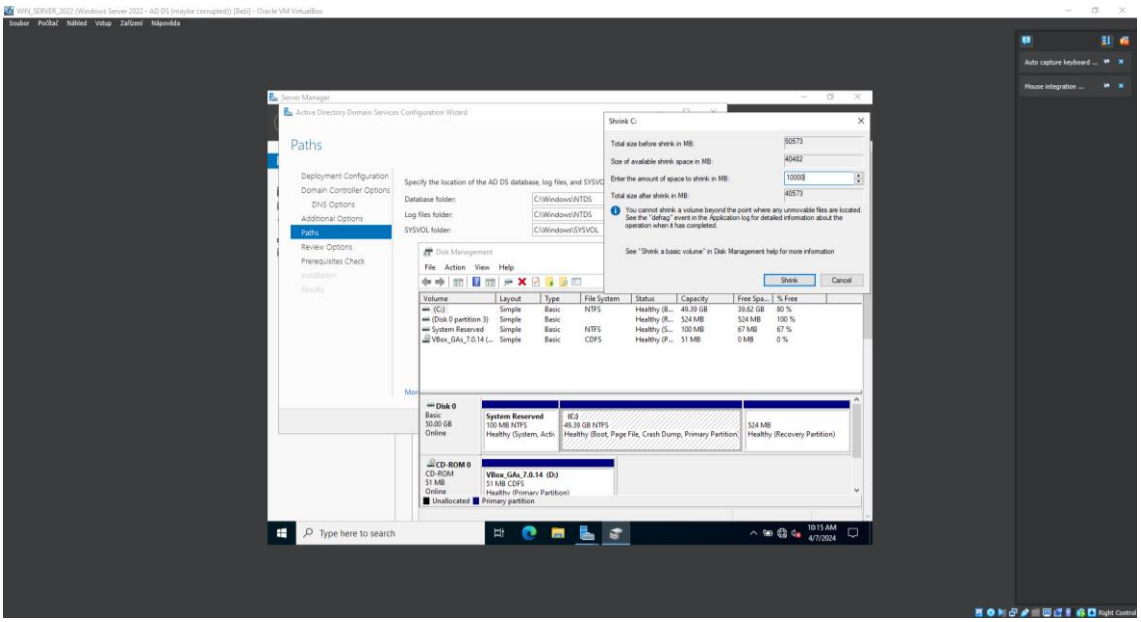
Když uživatel klikne na možnost Povýšit tento server na řadič domény otevře mu se průvodce konfigurací služby AD DS (Active Directory Domain Server). V první záložce průvodce si zvolí možnost Přidat novou doménovou strukturu a napíše název kořenové domény, zde využije název domény, který použili v rámci konfigurace DNS služby. Obrázek 36 vizualizuje nastavení konfigurace nasazení při povýšení server na řadič domény.



Obrázek 36 – Windows Server – Konfigurace nasazení. Zdroj: vlastní

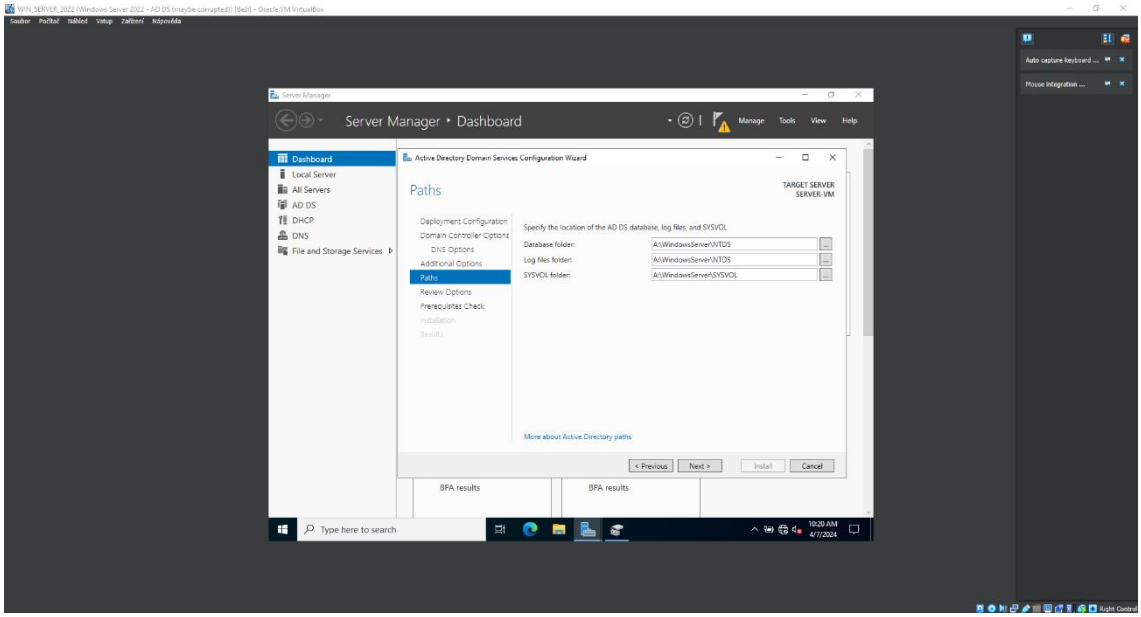
V možnostech řadiče domény se nebude nic měnit, jelikož to není potřeba. Ovšem uživatel zde zadá heslo pro případné obnovení adresářových služeb. V dalším kroku je možnost delegování DNS, avšak tuto možnost prozatím lze nechat vypnutou a pokračovat na další záložku Další možnosti. Tady lze vidět název domény pro rozhraní NetBIOS, který se automaticky doplní podle názvu kořenové domény. Ten byl zadán v první záložce Konfigurace nasazení. Na další záložce Cesty se nastavuje, kam se mají ukládat soubory služby Active Directory. Z Bezpečnostních důvodů by tyto cesty změněny na jiný disk nebo oddíl, než je základní oddíl C. Bohužel náš virtuální stroj má jenom jeden pevný disk, ale v rámci simulace lze vytvořit nový oddíl pro lepší odraz reality. Tento krok je možné vykonat během konfigurace služby Active Directory Domain Services. Když uživatel klikne pravým tlačítkem na ikonu Start, která se nachází v dolním levém rohu operačního systému, tak se mu otevře nabídka možností, kde si zvolí Správa disků. Klikne opět pravým tlačítkem na daný disk ve virtuálním stroji pro další kontextovou nabídku a možnost Zmenšit svazek…. Zadá požadovanou velikost kapacity pro zmenšení disku, takže v tom případě 10 GB. Tím se mu vytvoří volné místo, které není nikam přiřazené. Označí si ho a opět si otevře kontextovou nabídku, kde si zvolí možnost Nový jednoduchý svazek…. Projde průvodce vytvořením jednoduchého svazku, kde je důležité zadat jméno a označení svazku. Obrázek 37 zobrazuje zmenšení primárního

oddílu pro vytvoření nového oddílu, na kterém se budou ukládat soubory služby Active Directory Domain Services.



Obrázek 37 – Windows Server – AD DS Cesty a nová oddíl. Zdroj: vlastní

Po vytvoření nového oddílu je potřeba vytvořit stejnou souborovou strukturu na novém oddílu jako výchozí, která se nabízela vytvořit na pevném disku C. Obrázek 38 znázorňuje nově přidělené cesty pro soubory služby Active Directory Domain Services na novém oddílu.

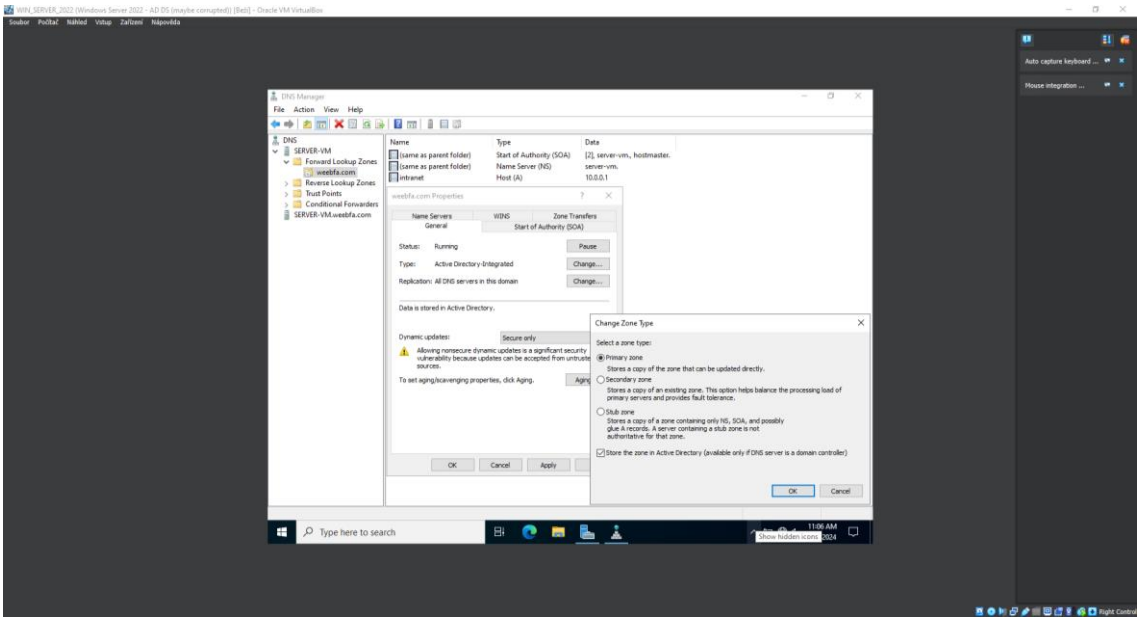


Obrázek 38 – Windows Server – AD DS nové cesty. Zdroj: vlastní

Následně se lze se proklikat průvodcem konfigurací služby AD DS (Active Directory Domain Server) až do bodu instalace služby AD DS. Po hotové instalaci se Windows Server automaticky restartuje a už při přihlášení lze vidět, že přihlašovací

údaje jsou zapsány v doménovém tvaru. Úspěšné přihlášení značí, že instalace služby Active Directory Domain Server proběhla úspěšně.

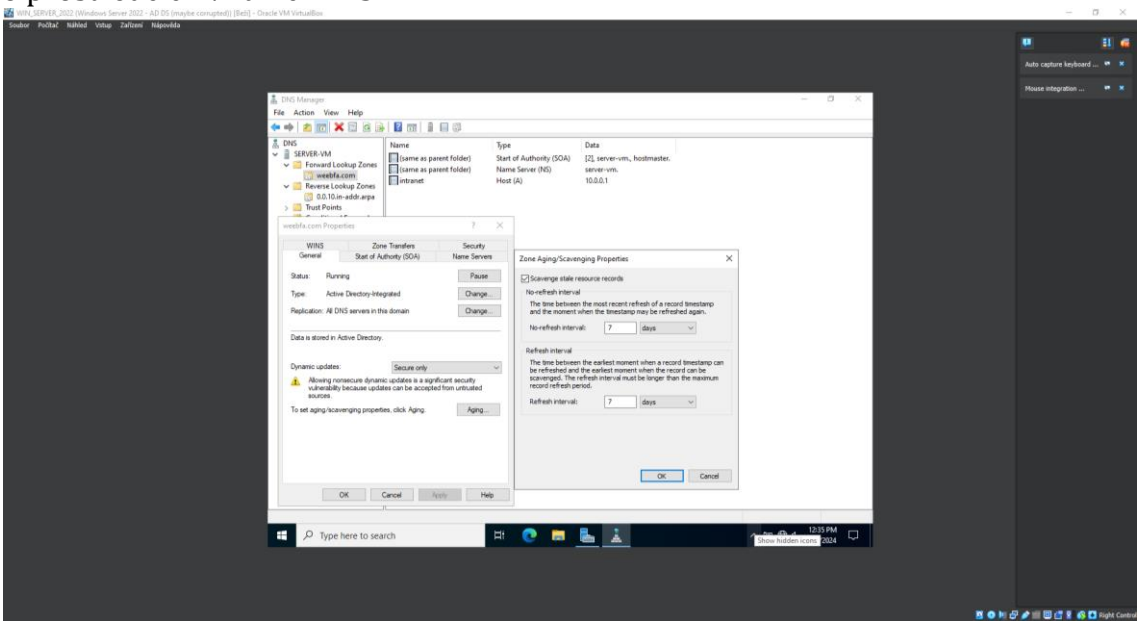
Po úspěšném nasazení AD DS je potřeba integrovat předešlé protokoly a služby pro zakomponování AD DS. Týká se to konkrétně DHCP a DNS. V rámci DNS je potřeba provést integraci. Integraci uživatel provede ve Správci DNS. Takže opět přes Správce serveru si otevře Správce DNS. V levém panelu klikne na možnost DNS a označí daný Windows Server pro otevření kontextové nabídky, kde klikne na Správce DNS. Rozbalí zóny dopředného vyhledávání a otevře kontextovou nabídku vytvořené zóny. Budou ho zajímat vlastnosti a u položky Typ klikne na tlačítko Změnit. Otevře se mu okno Změnit typ zóny a zde zaškrtne poslední možnost Uložit zóny do adresáře Active Directory. Při kliknutí na tlačítko OK mu vyskočí dialog, zda si opravdu přeje provést tyto změny, což uživatel potvrdí. Nyní může změnit nastavení Dynamické aktualizace na Pouze zabezpečené a Potvrdit. Totéž je potřeba udělat pro zónu zpětného vyhledávání, kde postup je zcela identický. Obrázek 39 znázorňuje integraci DNS ve Správci DNS a přepnutí nastavení pro dynamické aktualizace na bezpečné.



Obrázek 39 – Windows Server – DNS – Integrace. Zdroj: vlastní

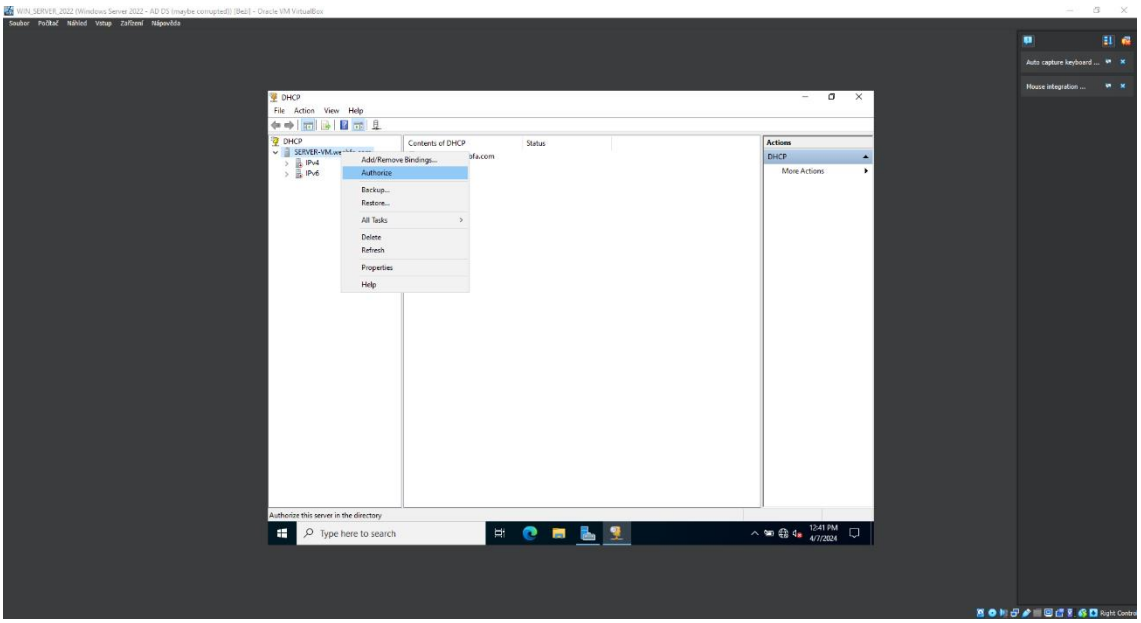
V rámci vlastností může nastavit ještě automatický úklid zastaralých DNS záznamů. Ve vlastnostech klikne na tlačítko Stárnutí a v okně Vlastnosti stárnutí a úklidu zastaralých dat zóny zaškrtne možnost Uklidit zastaralé záznamy o prostředcích. Toto natavení se provádí u dopředného, tak i u zpětného

vyhledávání. Obrázek 40 ukazuje možnost nastavení úklidu zastaralých záznamu o prostředcích v rámci DNS.



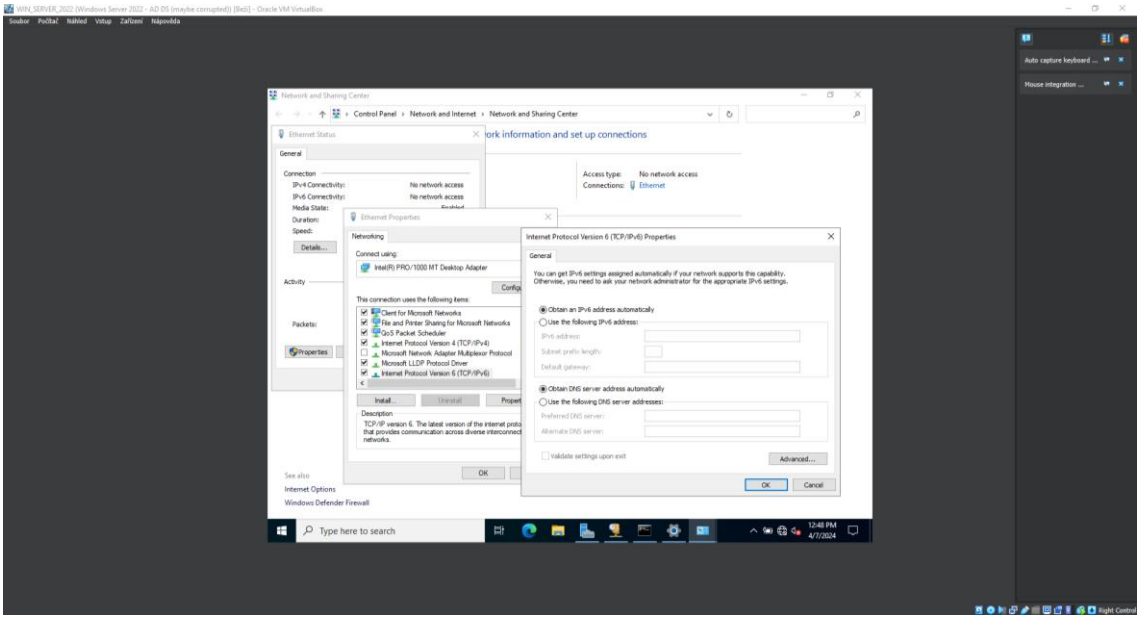
Obrázek 40 – Windows Server – DNS – Zastaralé záznamy. Zdroj: vlastní

Následně je nutné udělat autorizaci DHCP serveru. Ve Správci serveru si uživatel otevře Správce DHCP stejně jako Správce DNS, jen místo DNS klikne na možnost DHCP. Ve Správci DHCP otevře kontextovou nabídku daného serveru a klikne na možnost Autorizovat. Může se objevit hláška o potvrzení autorizace, ale nemusí. Ikony serveru by měly automaticky začít svítit zeleně nebo na ně stačí kliknout. Obrázek 41 představuje autorizaci DHCP serveru v rámci Active Directory.



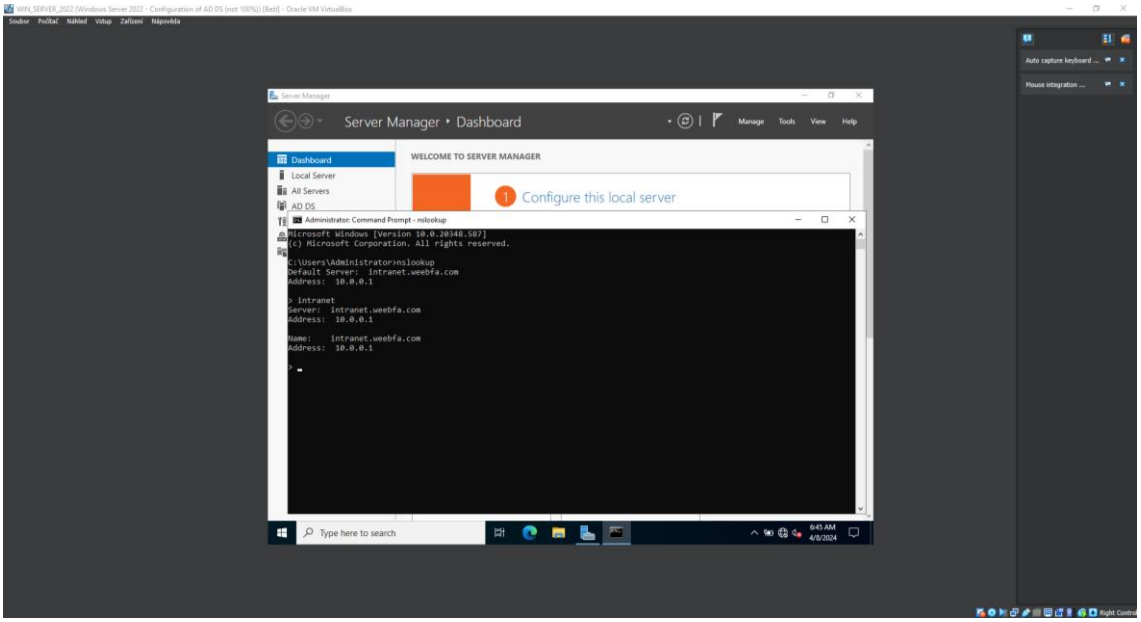
Obrázek 41 – Windows Server – DHCP – Autorizace. Zdroj: vlastní

Pro ověření dokončení konfigurace AD DS se využije opět příkaz nslookup v příkazové řádce. Na výstupu příkazu se mohou objevit dvě anomálie. První je chybová hláška o vypršení DNS. Pro odstranění této chybové hlášky stačí v nastavení adaptéru pro IPv6 přepnout získání DNS serveru na automatické obdržení DNS serveru. Obrázek 42 představuje možnost automatického obdržení DNS serveru v nastavení adaptéru pro IPv6.



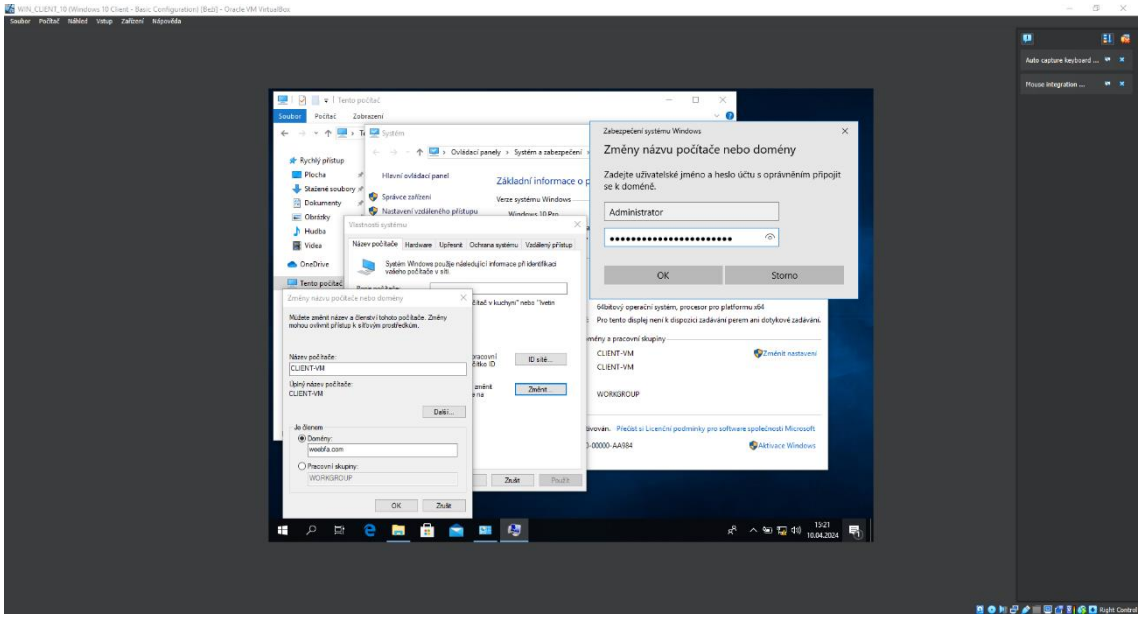
Obrázek 42 – Windows Server – DNS server pro IPv6. Zdroj: vlastní

Druhou je chybný překlad intranetu na IP adresu localhostu. Tu to chybu lze jednoduše vyřešit opět v nastavení adaptéru pro IPv4 a zkontrolovat Primární DNS server. Je možné, že po instalaci a konfiguraci AD DS se Alternativní DNS server nastavil jako primární a náš původní primární DNS server se už nebere v potaz. Po vyřešení těchto problémů by nslookup měl vrátit správný požadovaný výstup. Obrázek 43 zobrazuje požadovaný výstup příkazu nslookup.



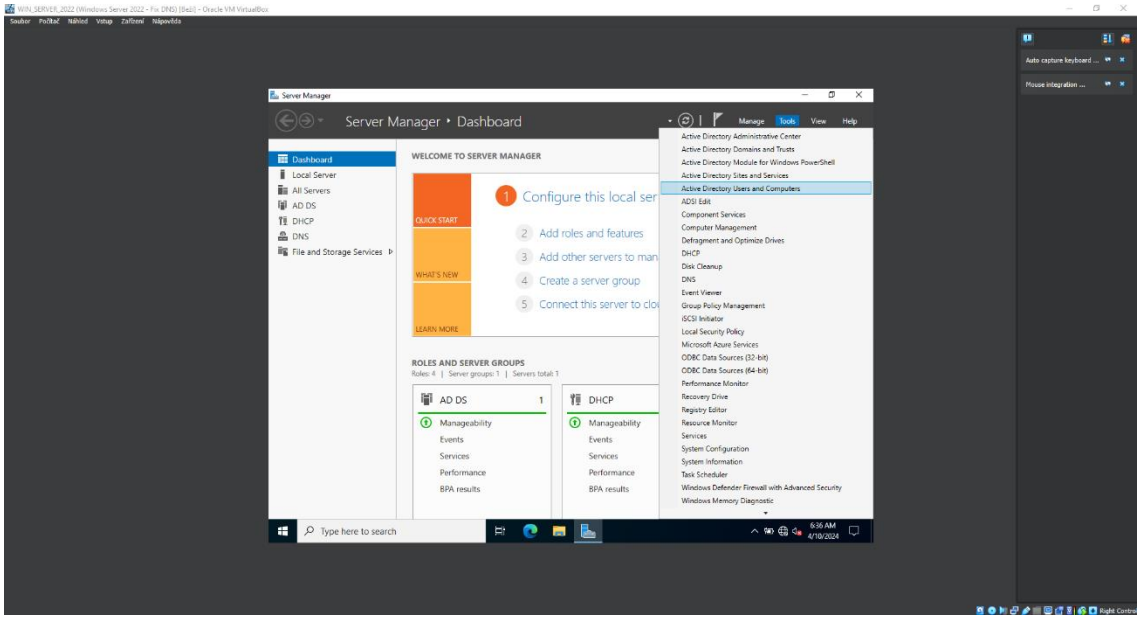
Obrázek 43 – Windows Server – Ověření funkčnosti AD DS. Zdroj: vlastní

Po úspěšném ověření fungování AD DS lze připojit klientský počítač do domény. Cesta k nastavení domény bude stejná jako přejmenování Windows klienta. Takže si uživatel otevře Průzkumníka souborů a v něm si otevře kontextovou nabídku položky Tento počítač a klikne na Vlastnosti. To mu otevře Ovládací panely a přehled systémových informací, zde u názvu počítače klikne na odkaz Změnit nastavení. Otevřou se mu Vlastnosti systému a jeho zajímá tlačítko Změnit, které mu otevře okno Změny názvu počítače nebo domény. Už z pojmů vyplývá, že cesta je správná. Zaškrtne políčko Je členem a zadá dané domény. Zde záleží na několika aspektech, protože připojení do domény je jedno z nejvíce záludných věcí na provedení. Avšak při správném postup by nemělo dojít k žádnému problému. Po kliknutí na tlačítko OK se objeví přihlašovací okno, kam stačí zadat přihlašovací údaje Administrátora Windows Serveru 2022. Po zpracovaní by se měla objevit hláška Vítejte v doméně. Následně lze nechat počítač restartovat. Při dalším přihlášení a změně přihlašovaného účtu si lze povšimnout, že klientský počítač vyžaduje doménové přihlášení. Obrázek 44 představuje postup, jak připojit Windows klienta do vytvořené domény.



Obrázek 44 – Windows Klient – Připojení do domény. Zdroj: vlastní

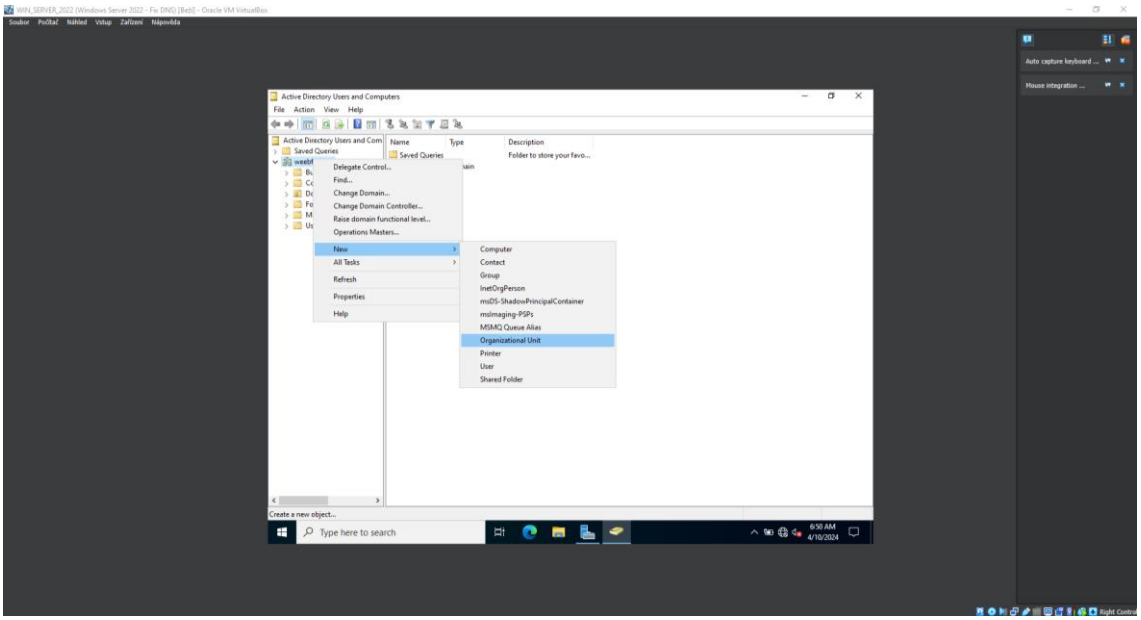
Nyní když už je Windows klienta připojený do dané domény bude potřeba vytvořit uživatelé, kteří se přes daného Windows klienta budou moci přihlásit. Ve Windows Serveru 2022 si uživatel otevře Správce serveru a nahoře vlevo položku Nástroje, zde si najde Uživatelé a počítače služby Active Directory. Obrázek 45 znázorňuje otevření nástroje Uživatelé a počítače služby Active Directory přes nástroje ve Správci Serveru.



Obrázek 45 – Windows Server – AD – Uživatelé a počítače. Zdroj: vlastní

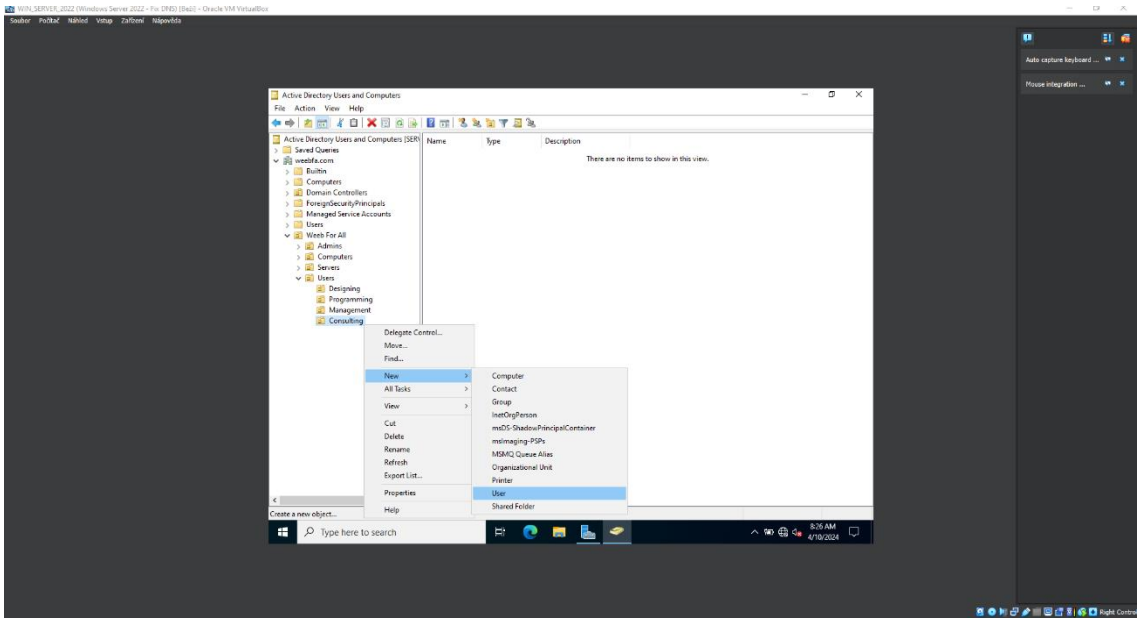
V navigátoru na levé straně si uživatel označí danou doménu pro otevření kontextové nabídky, vybere Nová položka a následně organizační jednotka. Tím si vytvoří jednotku reprezentující simulovanou firmu a v ním následně vytvoří

potřebné uživatele a skupiny podle představeného návrhu. Obrázek 46 ukazuje postup vytvoření organizační jednotky.



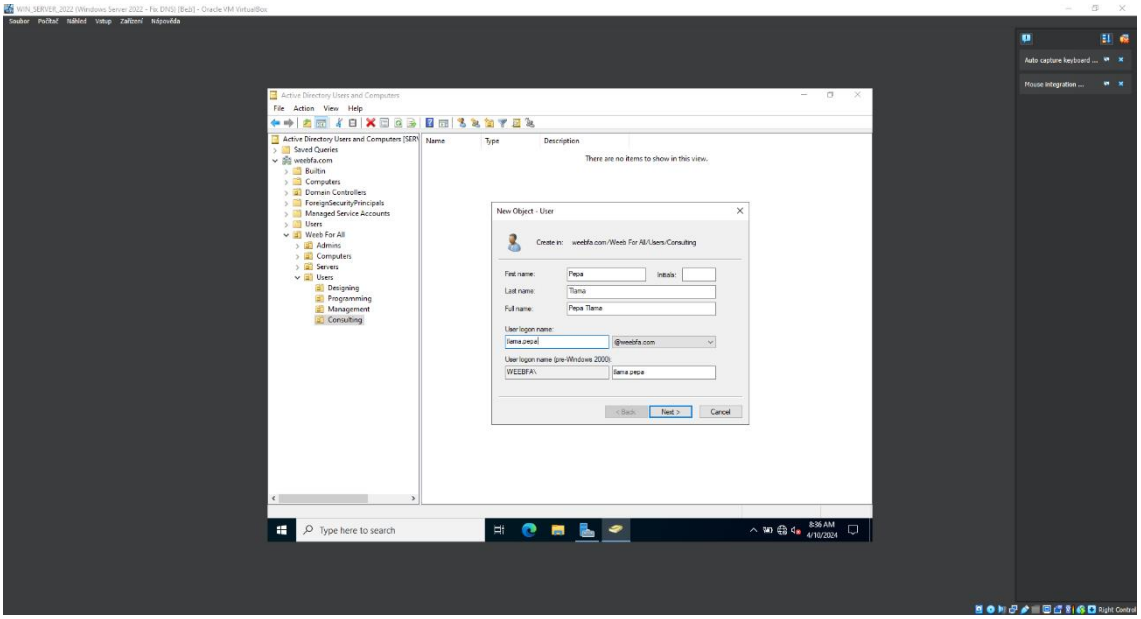
Obrázek 46 – Windows Server – AD – Organizační jednotka. Zdroj: vlastní

Při založení organizační jednotky se uživateli objeví okno, kam se zadává název dané organizační jednotky a také vidí políčko, které je už předem zaškrtnuté. Toto políčko zajistí ochranu objektu před náhodným odstraněním, kterou je doporučeno nechat zapnutou. V této organizační jednotce může tvořit organizační infrastruktury simulované firmy pomocí dalších Organizačních jednotek. Po vytvoření simulované organizační infrastruktury může vytvořit jednotlivé uživatele daných skupin. Když si označí danou organizační jednotku, kde chce vytvořit nového uživatele, a otevře kontextovou nabídku. V ní opět rozbalí položku Nová položka a možnost Uživatel. Obrázek 47 představuje vytvořenou organizační infrastrukturu dané simulované firmy a postup pro vytvoření uživatele.



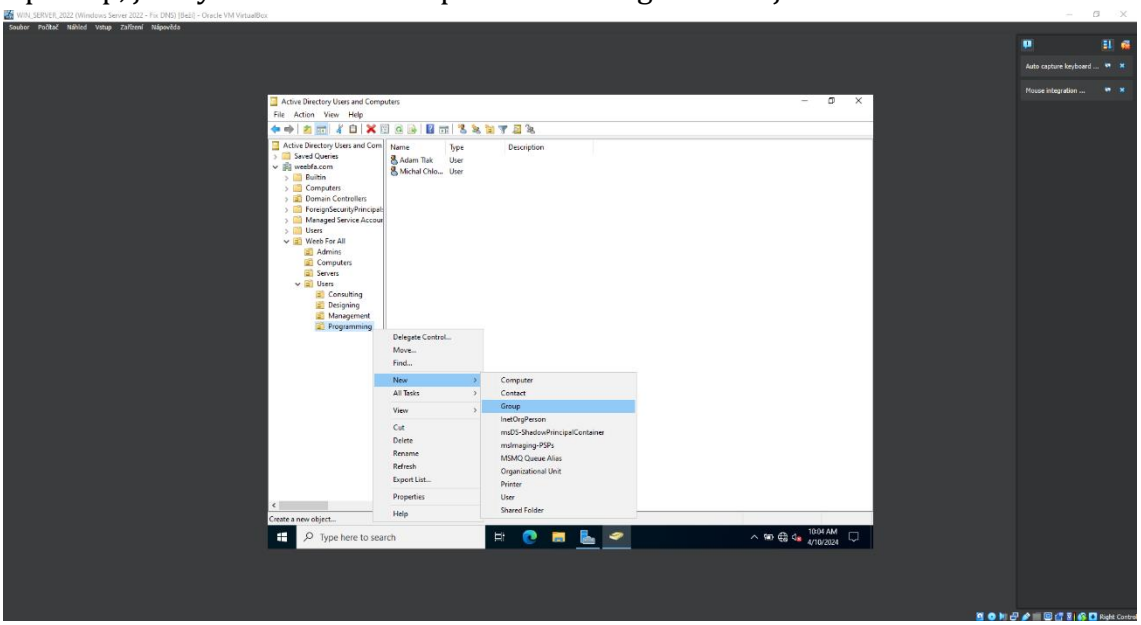
Obrázek 47 – Windows Server – AD – Vytvoření uživatele. Zdroj: vlastní

V nově otevřeném okně Nový objekt – Uživatel lze vidět vlastnosti uživatele, které jsou pro jeho vytvoření potřebné. Při standartním vyplnění Jména a Příjmení si lze povšimnout, že políčko pro Jméno a Příjmení se už samo vyplňuje podle hodnot, které se zadají u Jména a Příjmení. Pokud to není potřeba, tak Iniciály dalších jmen se nemusejí zadávat. Přihlašovací uživatelské jméno je poslední hodnotu, která se musí vyplnit. Existuje několik přihlašovacích formátů, v dané doméně byl využit běžný formát jmeno.prijmeni. Obrázek 48 vizualizuje nastavení vlastností uživatele.



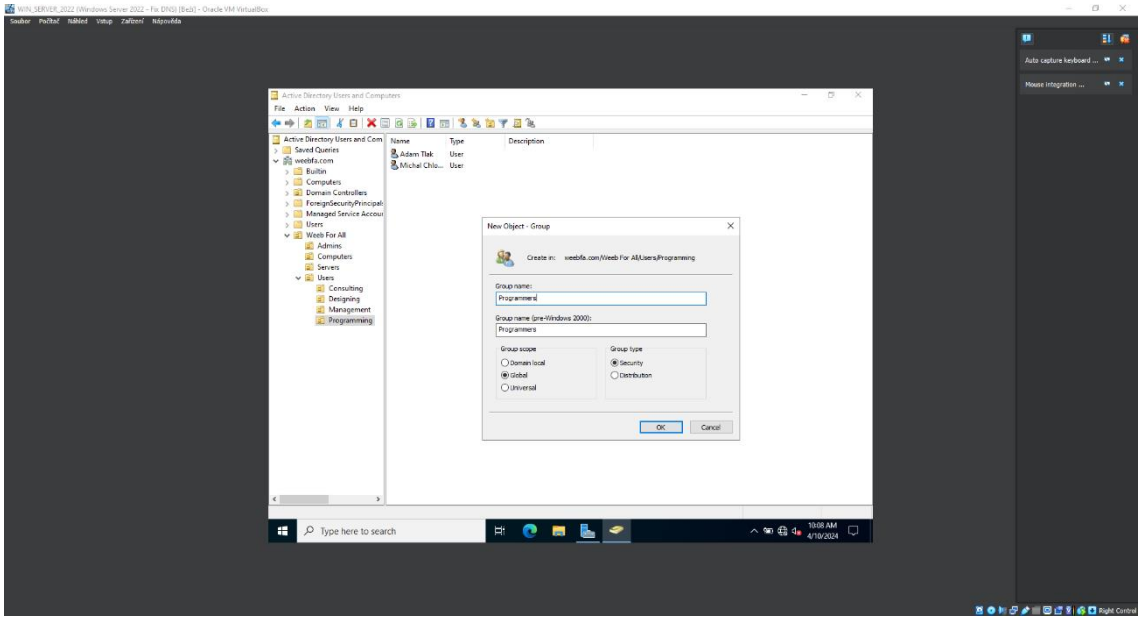
Obrázek 48 – Windows Server – AD – Login uživatele. Zdroj: vlastní

Po kliknutí na tlačítko Další uživatel je přesunut na nastavení hesla. Zde přidělí uživateli silné heslo a případně doplňující nastavení hesla. V tomto případě byly odškrtnuty všechny nastavení hesla, protože se nimi bude pracovat později v rámci Objektu skupinových zásad. Na konečném okně je shrnutí vlastností daného uživatele a tlačítko Dokončit, které dokončí tvorbu nového uživatele. Stejným způsobem se vytvoří další potřební uživatelé v rámci organizační infrastruktury. Když už jsou potřební uživatelé vytvoření v daných Organizačních jednotkách, lze k nim vytvořit příslušné skupiny. Stejně jako u Organizačních jednotek nebo u uživatelů, tvorba je identická. Kontextová nabídka dané organizační jednotky, Nová položka a Skupina. Obrázek 49 ilustruje vytvořené uživatele a postup, jak vytvořit novou Skupinu v dané organizační jednotce.



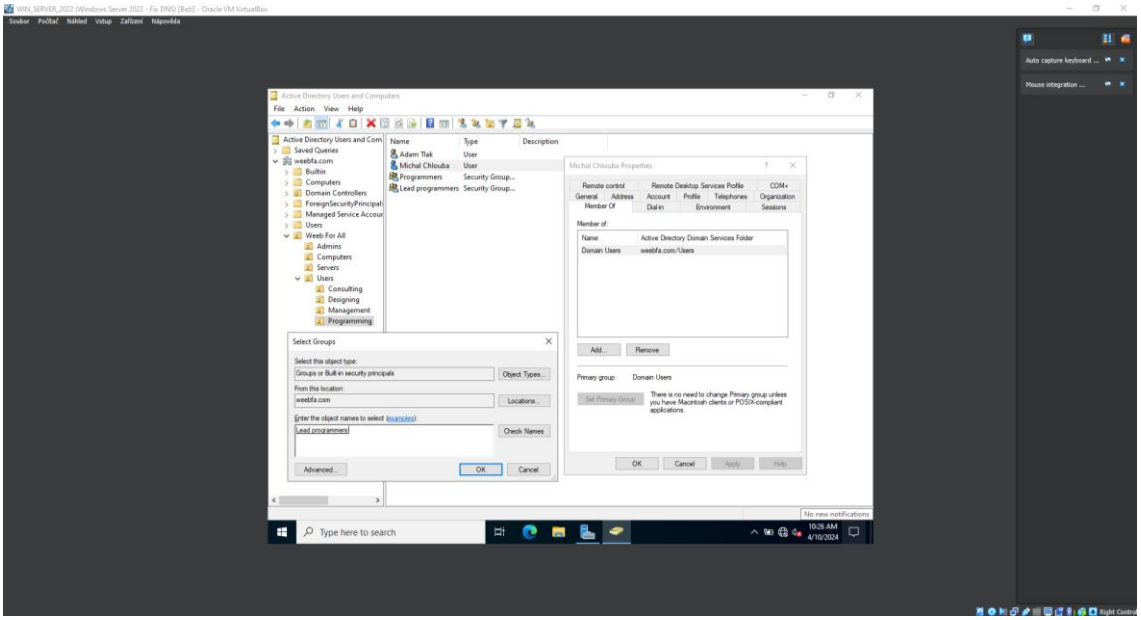
Obrázek 49 – Windows Server – AD – Vytvoření skupiny. Zdroj: vlastní

Zadání názvu skupina a potvrzení tlačítkem OK je všechno, co je potřeba udělat pro vytvoření nové skupiny. Obrázek 50 ukazuje okno s vytvořením skupiny, kde stačí zadat pouze název a potvrdit.



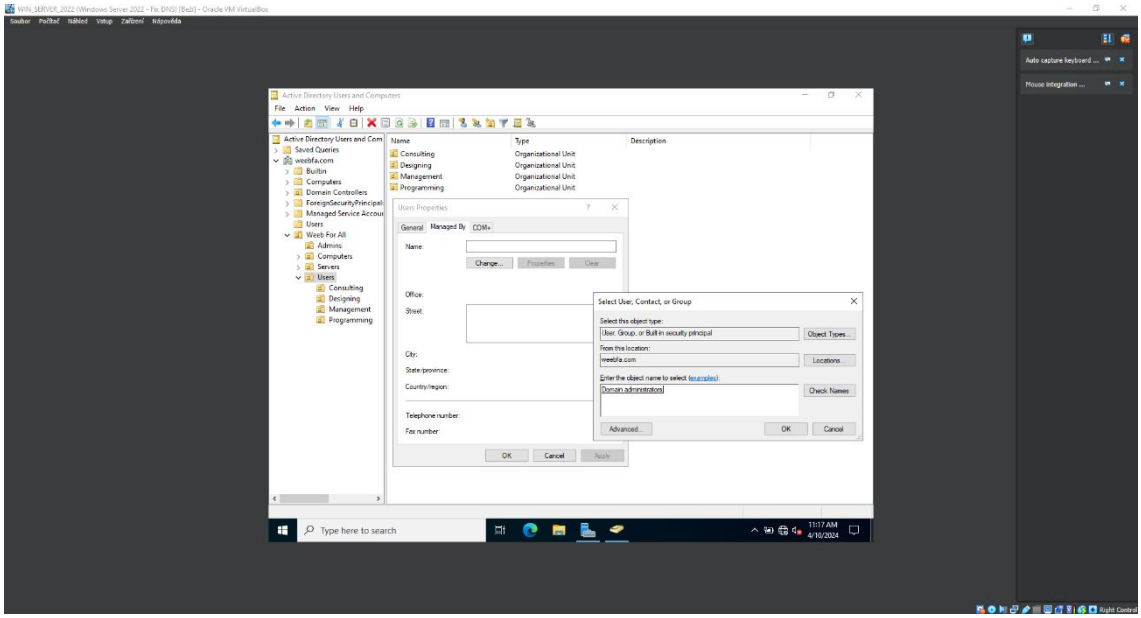
Obrázek 50 – Windows Server – AD – Název skupiny. Zdroj: vlastní

Tímto způsobem se vytvoří ostatní potřebné skupiny v rámci organizační infrastruktury. Jakmile bude stačit počet vytvořených skupin, tak už zbývá konkrétní uživatele přihlásit do daných skupin. Existují dva způsoby, jak přidat existující uživatele do skupin. Pro danou simulaci byl využit způsob, který je soustředěn na přidání jednoho konkrétního uživatele do skupiny. Uživatel si označí konkrétního uživatele pro otevření kontextové nabídky a následně klikne na Vlastnosti. Zde najde záložku Je členem a klikne na tlačítko Přidat. Otevře se mu okno Vybrat objekt typu: Skupiny a do dolní textové oblasti napíše název dané skupiny, kterou chce přiřadit. Aby si byl stoprocentně jistý, tak si název skupiny může ověřit tlačítkem Kontrola názvů. Když se název dané skupiny zvýrazní potržením, tak je název skupiny validní. Klikne na tlačítko OK a může vidět, že v tabulce Je členem přibyla přidaná skupina. Potvrdí změny tlačítkem Použít a spravovaný uživatele ke úspěšně přidělen ke skupině. Obrázek 51 zobrazuje postup přiřazení skupiny uživatelovi.



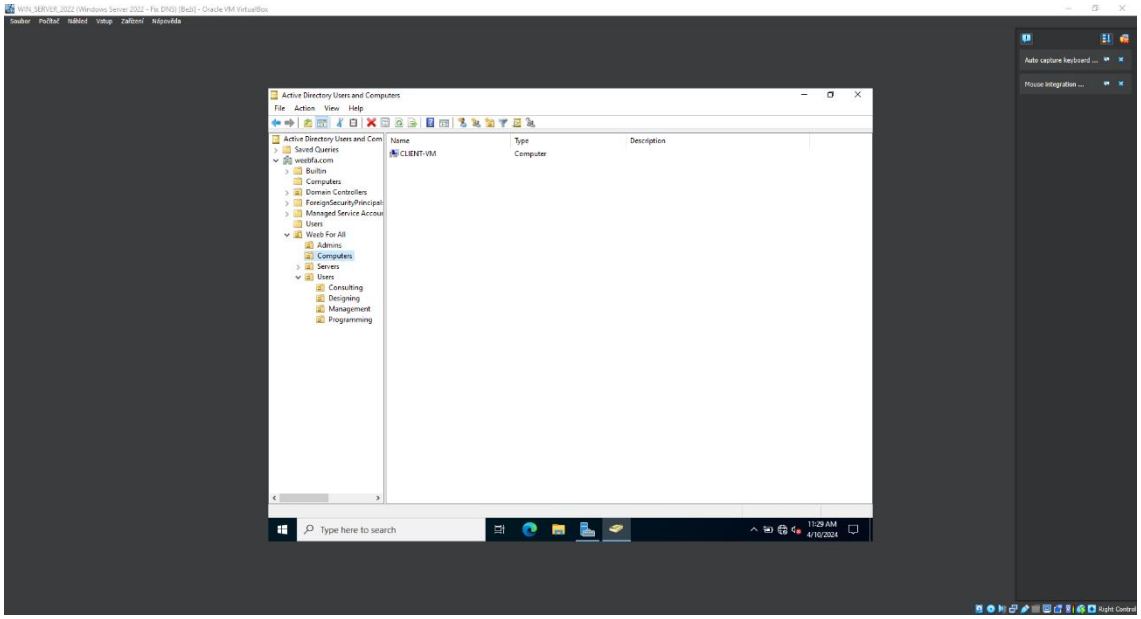
Obrázek 51 – Windows Server – AD – Uživatel ke skupině. Zdroj: vlastní

Následně je vhodné nastavit správce organizační jednotky. Pro tuto správu je vhodné dát pověření administrátoru. Nejedná se o lokálního administrátora Windows Serveru, ale nejlépe o vytvořeného uživatele, který bude spravovat danou doménu. Takže v simulované organizační infrastruktuře je požadující takového uživatele vytvořit a zároveň vytvořit i skupinu Správci domény, kam se poté daný uživatele zařadí. Po vytvoření uživatele i skupiny lze ho nastavit jako správce pro danou organizační jednotku Uživatelů. Uživatel si označí danou organizační jednotku a otevře kontextovou nabídku, kde ho zajímají opět Vlastnosti. V novém okně přejde na záložku Správce objektu, zde klikne na tlačítko Změnit. To mu otevře okno, kde je žádáno zadání názvu objektu k výběru pro správu. Zde napíše nedávno vytvořenou skupinu Správci domény a nechá zkontrolovat název tlačítkem Kontrola názvu. Po úspěšné kontrole potvrdí změny a daná organizační jednotka má přiřazeného správce. Obrázek 52 představuje přidání správce pro organizační jednotku.



Obrázek 52 – Windows Server – AD – Přiřazení správce OJ. Zdroj: vlastní

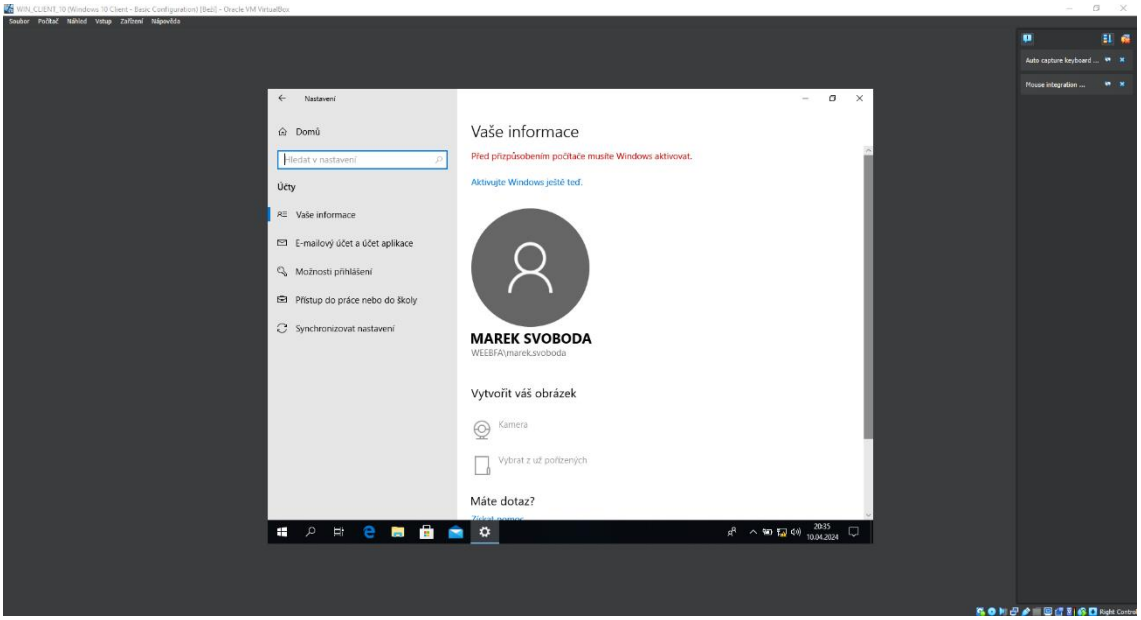
Jako poslední věc lze přiřadit Windows klienta přímo do doménové organizační jednotky. Pokud daný Windows klienta bude využíván jen pro danou domény, tak dané přiřazení specifikujeme Windows Serveru tuto skutečnost. Stačí Windows klienta přetáhnout z předdefinovaného adresáře Computers do dané organizační jednotky. Obrázek 53 reprezentuje úspěšně přemístění Windows klienta do dané organizační jednotky.



Obrázek 53 – Windows Server – AD – Přesunutí klienta do OJ. Zdroj: vlastní

Dalo by se říci, že v rámci uživatelů a počítačů Active Directory je nastavené a lze se nyní přihlásit pod nějakým vytvořeným uživatelem. Ovšem daný uživatel nebude mít zatím nastavená žádná specifická privilegia, bude se chovat jako klasický

uživatel bez omezení. Obrázek 54 vizualizuje přihlášeného uživatele ve Windows klientu, který byl vytvořen přes nástroj Uživatelé a počítače služby Active Directory.



Obrázek 54 – Windows Klient – Přihlášení AD uživatele. Zdroj: vlastní

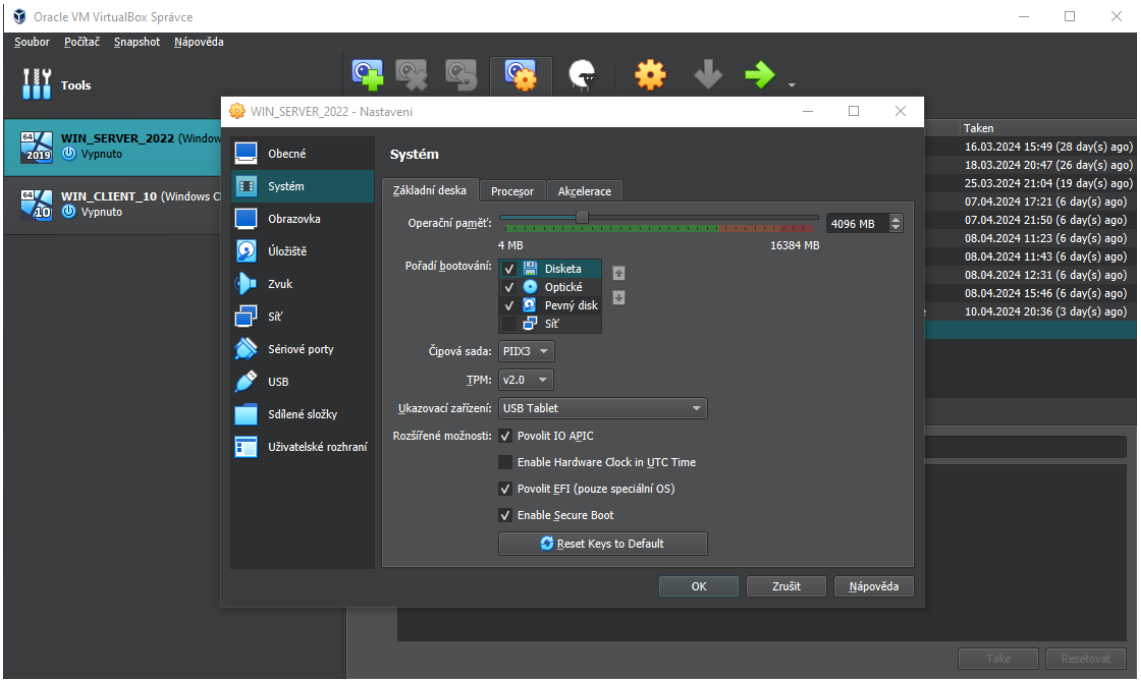
6.7 Hardening

Po veškeré přípravě virtuálních strojů až po vytvoření uživatelských účtů přes Active Directory se v následující kapitole budou probírat praktické zásady nasazení hardeningu. Veškeré zásady nasazení hardenigu by měl zpracovávat správce dané sítě.

6.7.1 Nastavení BIOSu

První zásadou je nastavení BIOSu, což se projevuje hned po zapnutí počítače. BIOS řídí chování mezi softwarem a hardware. Avšak v rámci hardeningu jsou dvě důležité položky, které je potřeba nastavit. První položkou je Secure Boot, který už z názvu chrání počítač před malware při zapnutí počítače. A druhým nastavením je zaheslování BIOSu, ať běžný uživatel k němu nemá přístup. Bohužel v rámci BIOS tuto složku nelze nasimulovat, protože BIOS se vztahuje na fyzické zařízení, a ne na virtuální stroje, které používají prostředky počítače, na kterém běží. Hlavní cestou, jak se dostat do BIOSu je stisknutí příslušné klávesy při zavádění počítače. Ta to klávesa se liší podle výrobce základní desky, avšak existují i systémové cesty, které nejsou závislé na výrobci desky. Mezi takové cesty patří spuštění příkazové řádky jako správce a zadání příkazu shutdown /r /fw /t 1. Po odklepnutí toho

příkazu se počítač vypne a zavede se do nastavení BIOSu. Složka /r reprezentuje restart, složka /fw reprezentuje firmware (BIOS) a složka /t 1 reprezentuje dobu po restartu. V BIOSu je potřeba vyhledat sekci zabezpečení a zde by má nacházet nastavení Secure Bootu a i nastavení hesla do BIOSu. Opět záleží na výrobci základní desky a verzi BIOSu, kde se tyto nastavení nacházejí. V rámci VirtualBoxu lze nastavit pouze Secure Boot přes nastavení daného virtuálního stroje. Uživatel si otevře natavení a v levém panelu vyhledá možnost Systém. Zde vidí nastavení Základní desky. Pro povolení Secure Bootu, který je normálně zašedlý musí zvolit verzi čipové sady. Pokud je nainstalován operační systém Windows 11 musí se zvolit verze 2.0, avšak pro Windows 10 lze zvolit i verzi 1.2. V tomto případě lze zvolit novější verzi 2.0. Ovšem možnost Secure Bootu je stále zašedlá a dokud se nezaškrtne i možnost Povolit EFI (pouze pro speciální OS), tak tato možnost zůstane zašedlou. Obrázek 55 ukazuje postup pro povolení a nastavení Secure Bootu ve VirtualBoxu.

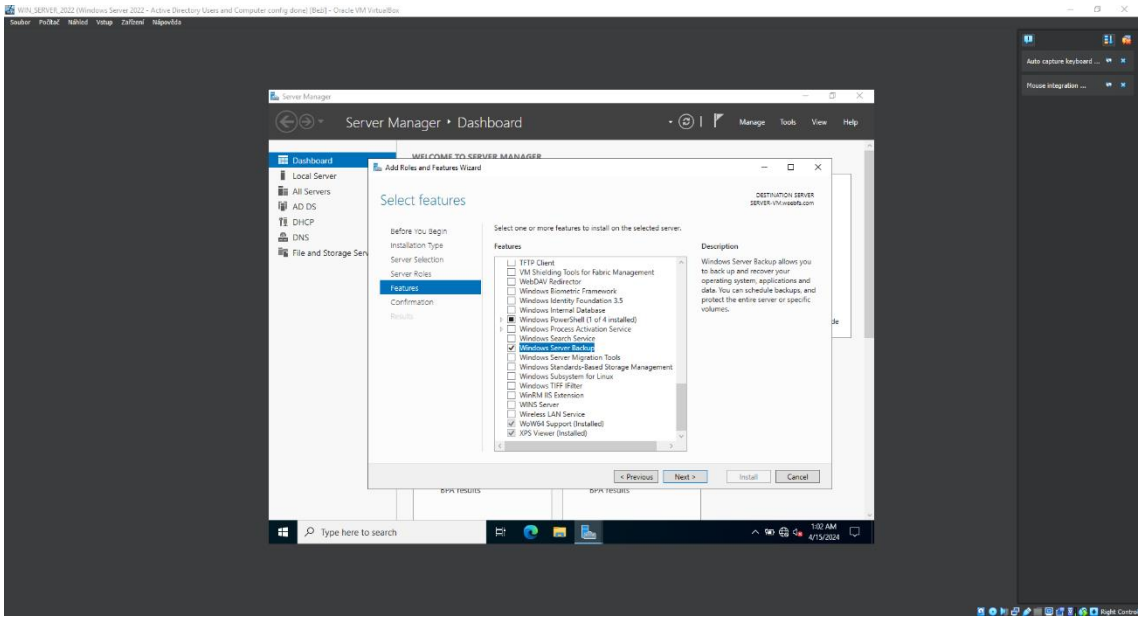


Obrázek 55 – VirtualBox – Nastavení Secure Bootu. Zdroj: vlastní

6.7.2 Zálohování dat

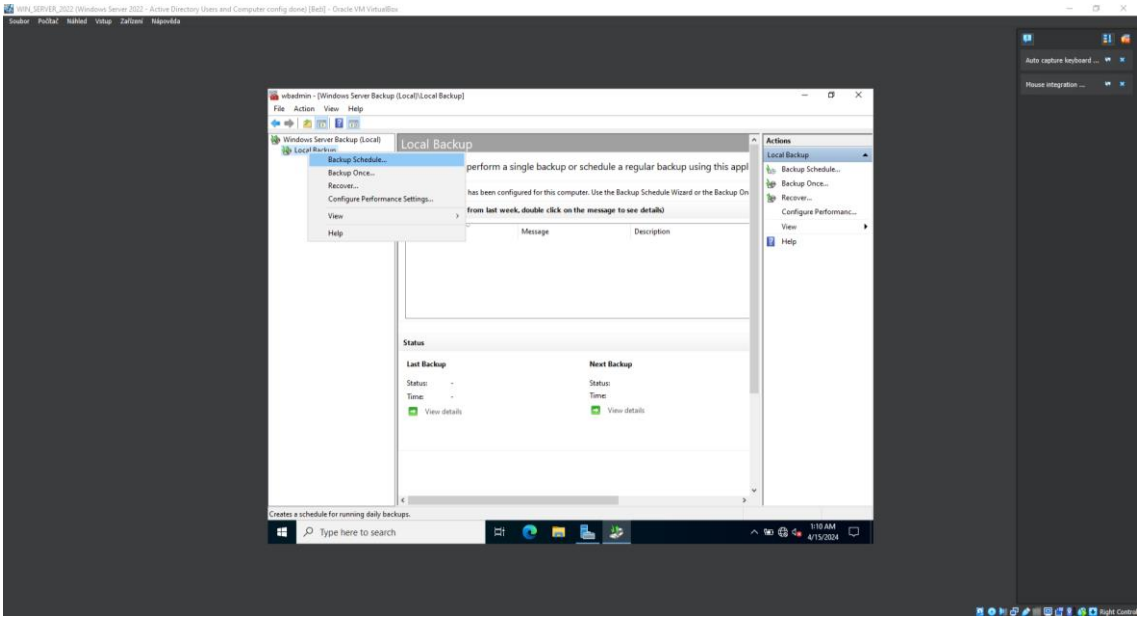
Zálohování dat je jedním typem řešení při ztrátě dat, protože ztracená data lze jednoduše obnovit přes zálohu. Windows Server 2022 je obdařen funkcí Windows Server Backup, která dokáže obnovit systémové obrazy, data a aplikace.

Avšak aby tato funkce mohla být využita, je potřeba ji nejdříve nainstalovat a nakonfigurovat na Windows Server 2022. Ve Windows Serveru 2022 si uživatel otevře Správce serveru a hned na hlavním panelu klikne na Přidat role a funkce. Stejným postupem jako u DHCP a DNS se prokliká až k položce Funkcím a vybere Windows Server Backup. Obrázek 56 zobrazuje vybrání Windows Server Backup.



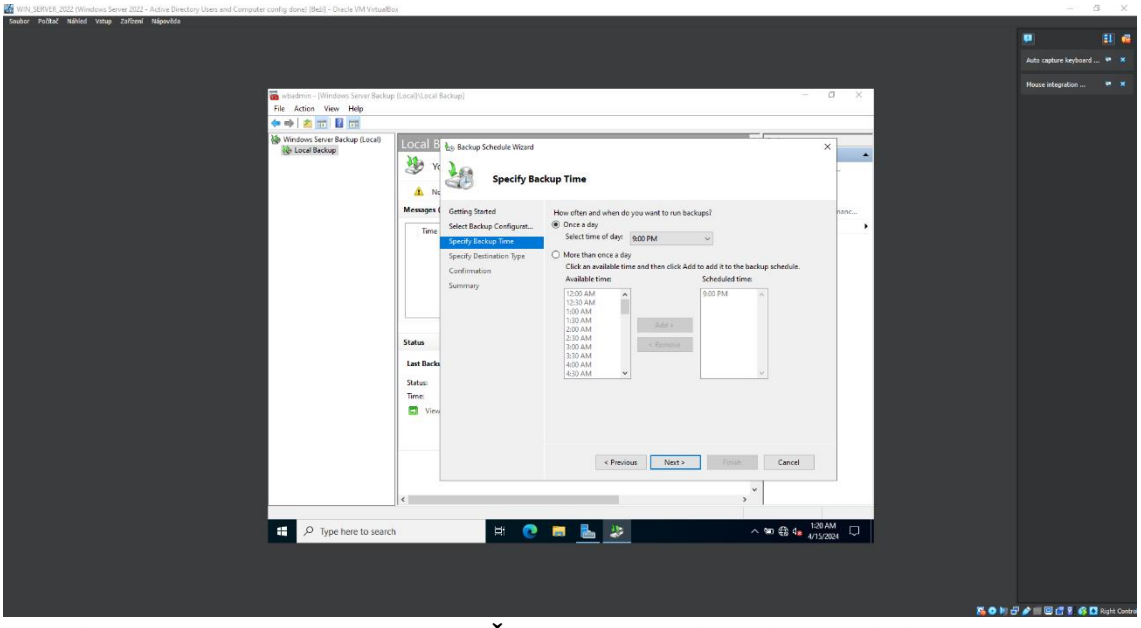
Obrázek 56 – Windows Server – Windows Server Backup. Zdroj: vlastní

Prokliká průvodce přidání rolí a funkcí až k samotné instalaci. Poté co instalace doběhne je několik možností, jak pracovat se zálohováním. Ovšem nejideálnější bude nastavit pravidelné zálohování, díky němuž uživatel nemusí myslet na provádění manuálního zálohování. Pro nastavení pravidelného zálohování je potřeba ve Správci serveru v pravém horním panelu vybrat Nástroje a v nich Windows Server Backup. Otevře se aplikace wbadmin – [Windows Server Backup (Local)\Local Backup]. Je možné, že aplikace se bude chvilku načítat, než zobrazí aktuální informace. Uživatel klikne v levém bočním panelu na položku Místní Zálohování pro otevření kontextové nabídky a vybere možnost Pravidelné Zálohování…. Obrázek 57 vizualizuje postup, jak otevřít průvodce pro Pravidelné zálohování.



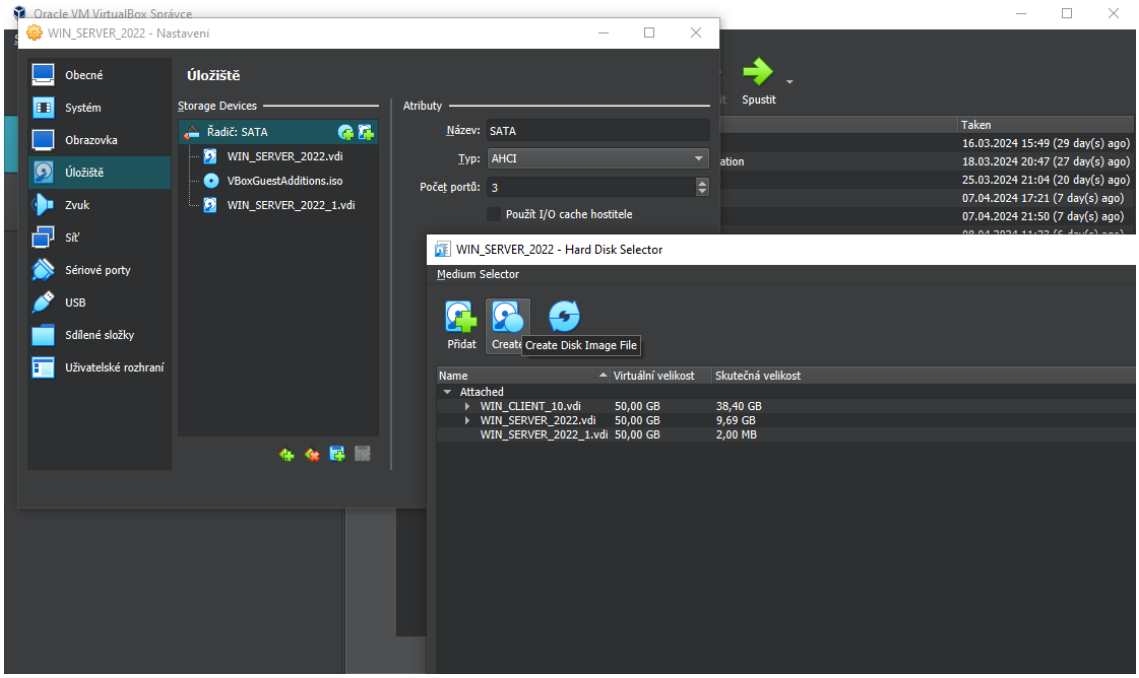
Obrázek 57 – Windows Server – Plánování Zálohování. Zdroj: vlastní

V průvodci Pravidelného Zálohování pokračuje na další okno kliknutím tlačítka Další. Na následujícím okně si uživatel může vybrat, zda chce zálohovat celý server nebo jenom konkrétní oddíly nebo soubory. V tomto případě se pokračovalo možností Celý server. Na další kartě ho čeká hlavní nastavení, a to kdy chce provádět pravidelné zálohy. Lze je nastavit jednou každý den v konkrétní den, nebo několikrát denně. Toto nastavení času by mělo odpovídat komplexnosti a potřeby zálohy daného Windows Serveru. Obrázek 58 zobrazuje možnosti nastavení času pro Plánování zálohování v rámci Windows Server Backup funkce.



Obrázek 58 – Windows Server – Čas pravidelného zálohování. Zdroj: vlastní

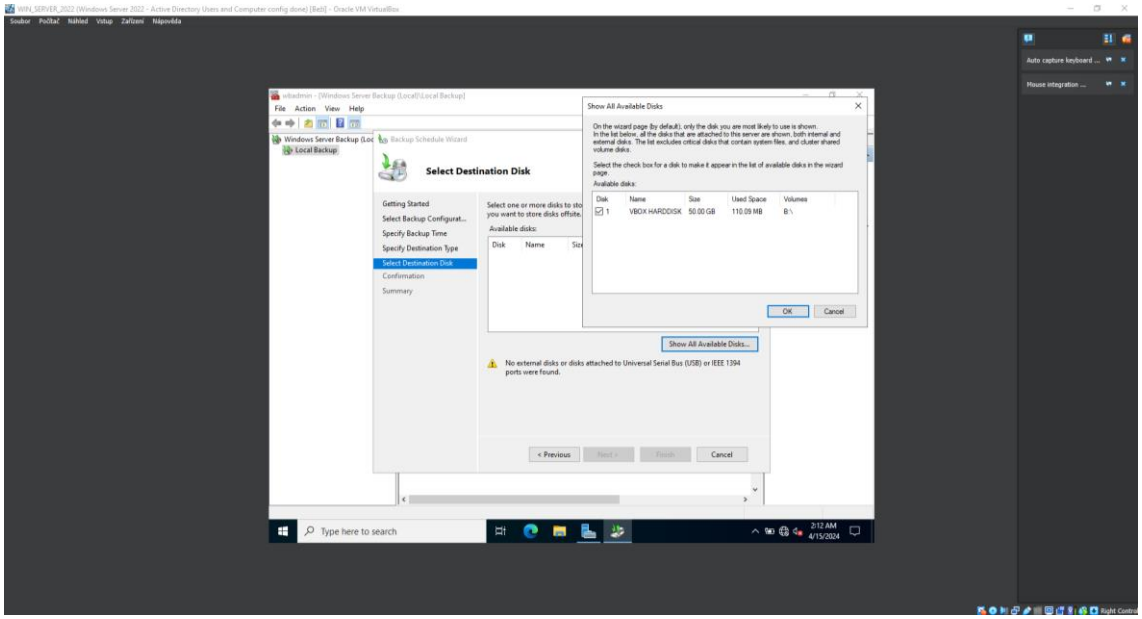
Na dalším okně je volba cílového úložiště. Jsou zde celkem tři možnost vybrání úložiště: Zálohování na pevný disk, který je určen k zálohování; Zálohování na oddíl a Zálohování na sdílenou složku. V tomto případě zálohovat na další oddíl nepůjde, jelikož původní disk už byl rozdělen na dva oddíly. Sdílené složky se nevytvářeli a v rámci bezpečnosti se jedná o nejméně bezpečné řešení. Takže podle kapitoly Bezpečnostní metody byla využita možnost uložení na pevný disk, který k tomu bude určen. Bohužel v tomto bodě simulace není dostupný další disk, protože při přípravě virtuálních strojů byl zaveden pouze jeden. To lze po vypnutí virtuálního stroje Windows Serveru 2022 v nastavení okamžitě napravit. Uživatel si otevře položku Úložiště a klikne na ikonku, která je reprezentována disketou se zelenám plusem. Otevře se mu Hard Disk Selector, zde klikne na ikonu Create a projde průvodce pro přidání pevného disku. Po dokončení průvodce se mu disk zobrazí v tabulce, tak ho vybere a stiskne tlačítko Choose, tím ho přiřadí danému virtuálnímu stroji. Obrázek 59 ukazuje postup, jak ve VirtualBoxu vytvořit a přidat nový pevný disk pro dané virtuální zařízení.



Obrázek 59 – VirtualBox – Přidání pevného disku. Zdroj: vlastní

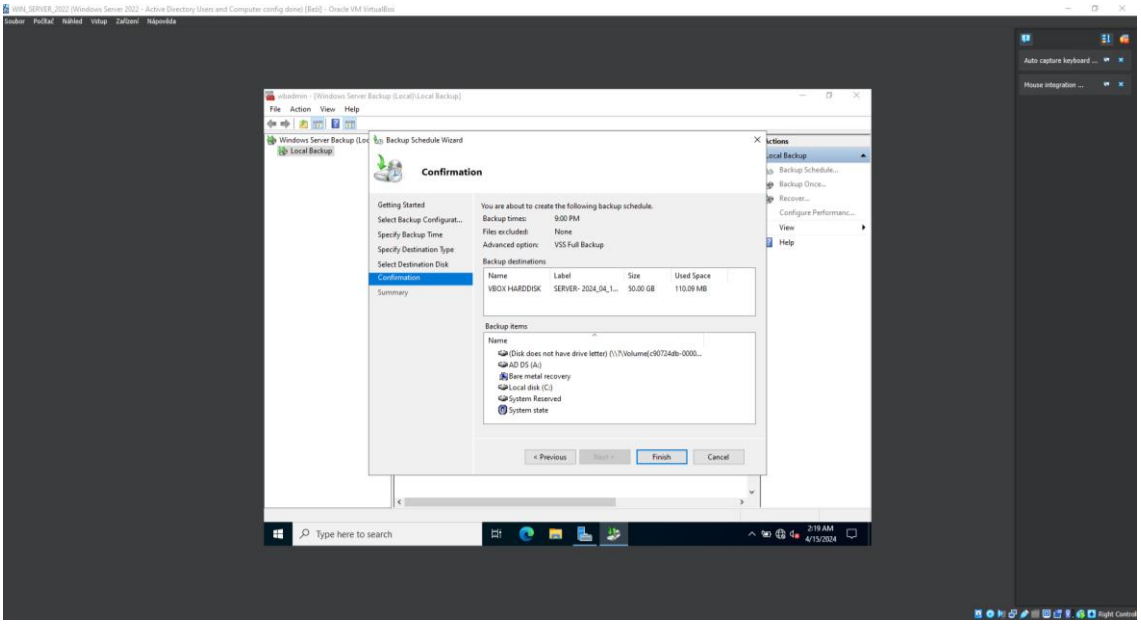
Když už byl nový disk přidán, tak se lze vrátit zpět k vytvoření Plánování zálohování s volbou uložit na daný disk. Po spuštění Windows Serveru 2022 se mohou objevit různé chyby, ovšem tyto chyby se tykají nově zavedeného disku, který není plnohodnotně integrován. Uživatel si otevře Správa disku. Hned

při otevření programu by na něj měla vyskočit tabulka s inicializací vytvořeného disku. Jedná se o vybrání schéma MBR nebo GPT daného disku. Jelikož daný disk bude využíván na zálohy, tak je lepší využít zde GPT. Nyní lze disk naformátovat a připravit pro použití. Bude mu přiřazeno písmeno B a název Backup. Když se uživatel prokliká opět k možnostem úložiště zálohy nechá první možnost a pokračuje dále. Vidí prázdnou tabulku, která značí, že zde není na výběr dostupný disk pro zálohu. Klikne na tlačítko pro zobrazení všech dostupných disků a vybere nově přidaný disk B. Po vybrání a potvrzení volby, daný disk se už nachází v tabulce dostupných disků. Tudíž ho lze vybrat a pokračovat dále. Obrázek 60 naznačuje výběr nového pevného disku pro plánované zálohování.



Obrázek 60 – Windows Server – Zvolení disku pro zálohu. Zdroj: vlastní

Jelikož disk B byl naformátován jako standartní typ disku pro běžné použití, tak se průvodce Plánování Zálohování zeptá, zda může disk naformátovat pro správné zálohování. Zde stačí všechno odsouhlasit a dostat se ke konečnému oknu se souhrnem zálohy. Obrázek 61 zobrazuje souhrn nastavení pravidelné zálohy.



Obrázek 61 – Windows Server – Potvrzení plánované zálohy. Zdroj: vlastní

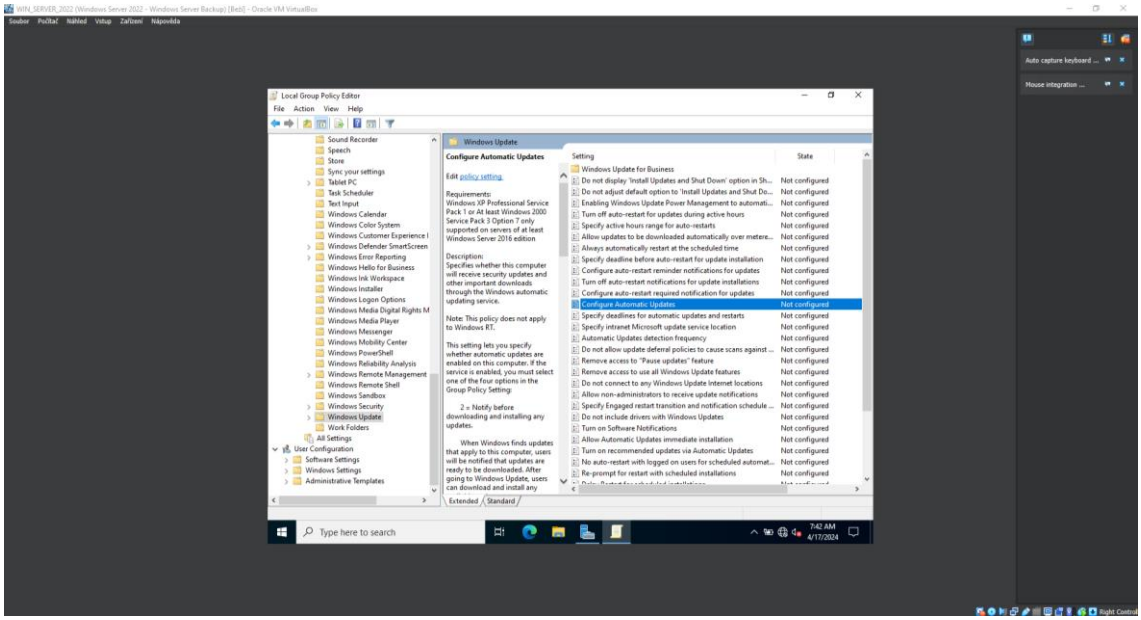
Tím to způsobem byla dokončena konfigurace pravidelné zálohování a v případě obnovy stačí se opět dostat k aplikaci wbadmin – [Windows Server Backup (Local)\Local Backup] a zvolit možnost Obnovit a následně postupovat podle průvodce Obnovy.

6.7.3 Automatické aktualizace

Nastavení automatických aktualizací je jednou z nejzásadnějších zásad nasazení hardeningu, protože udržují definice kybernetických hrozeb aktuálními. Automatické aktualizace lze nastavit pro samotný Windows Server 2022 i pro připojené Windows klienty.

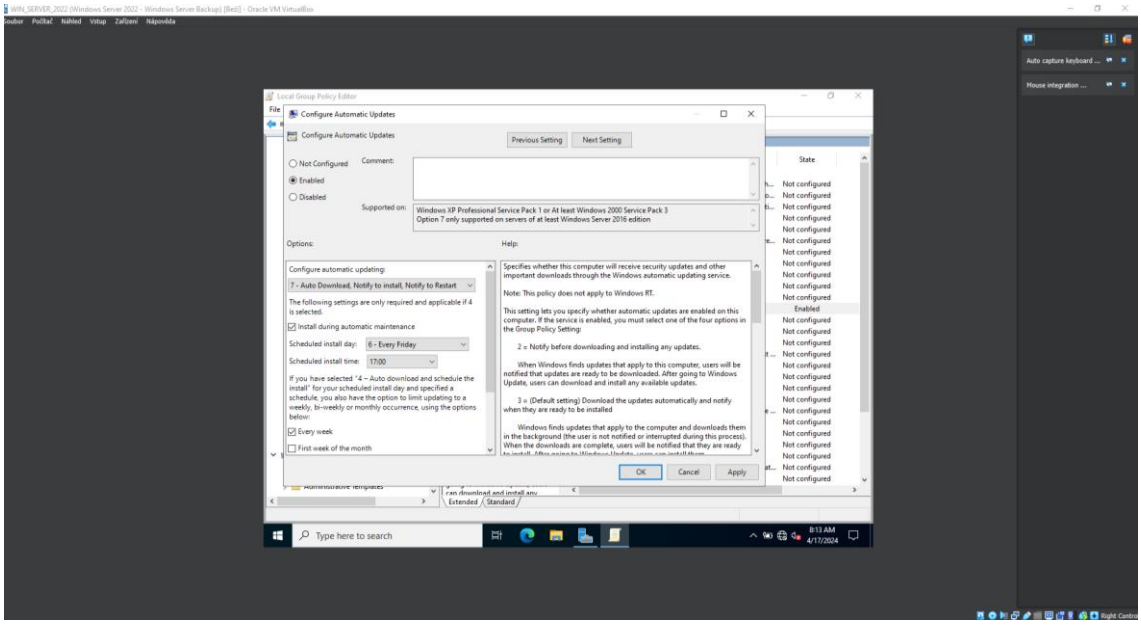
6.7.3.1 Windows Server aktualizace

Nastavení automatických aktualizací pro Windows Server 2022 je velice jednoduchý proces, který spočívá v otevření Editoru místních zásad skupiny. V levém bočním panelu rozbalit složku Šablony pro správu v kategorii Konfigurace počítače. Následně pokračovat do složky Součásti systému Windows a zde kliknout pro zvýraznění na složku Windows Update. V hlavním panelu se zobrazí několik položek, ovšem klíčová je položka Konfigurace automatických aktualizací. Obrázek 62 zobrazuje cestu ke konfiguraci automatických aktualizací pro Windows Server 2022 v Editoru místních zásad skupiny.



Obrázek 62 – Windows Server – Automatické aktualizace. Zdroj: vlastní

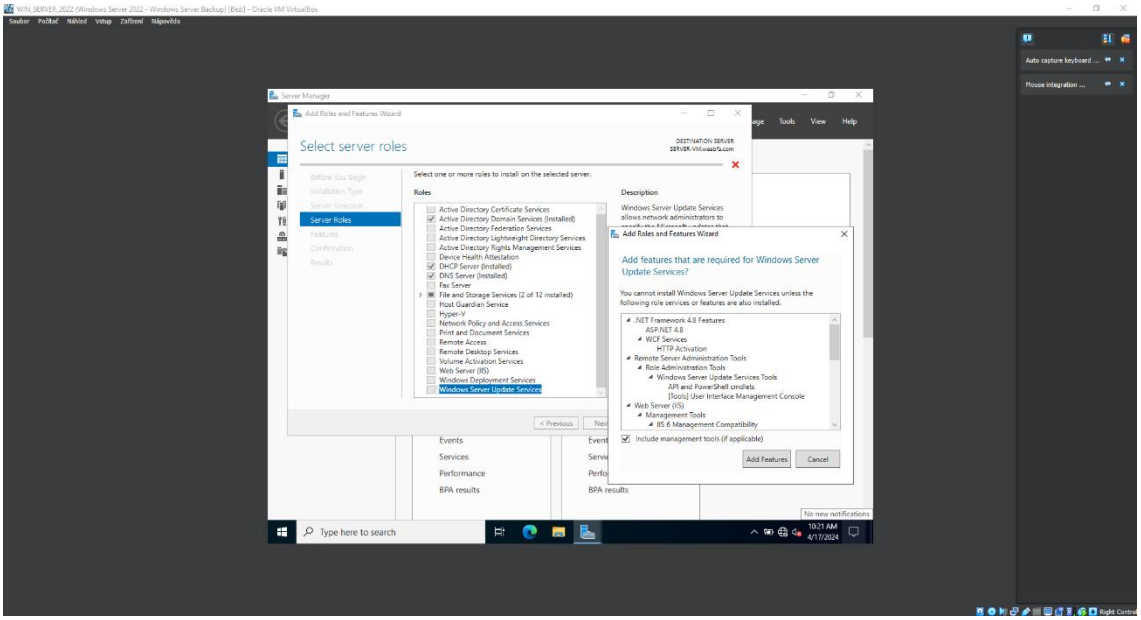
Když se na položku Konfigurace automatických aktualizací dvakrát klikne, otevře se nastavení této konfigurace. Pro potvrzení a aktivaci této konfigurace je důležité ji povolit. Uživatel může zvolit několik variací konfigurace: Upozorňovat na stažení a automatickou aktualizaci; Automaticky stahovat a upozorňovat na instalaci; Automaticky stahovat a plánovat instalaci; Povolit místnímu správci změnit nastavení a Automaticky stáhnout, upozornit na instalaci, upozornit na restartování. Už z jejich názvů je jasné, jak fungují. Ovšem vybrání správné variace spočívá na uživatelských preferencí. V rámci simulace byla vybrána poslední možnost. Také se zaškrtla možnost Instalovat během automatické údržby pro ucelenost údržby. Ostatní parametry času se nastavují, pokud uživatel zvolí možnost Automaticky stahovat a plánovat instalaci. Jedná se o upřesnění času a pravidelnosti instalace aktualizací. Po kompletní konfigurace automatických aktualizací stačí kliknout na tlačítko Použít a tím se konfigurace aktivuje a její stav v Editoru místních zásad skupiny se změní na Povoleno. Obrázek 63 představuje konfiguraci automatických aktualizací na Windows Serveru.



Obrázek 63 – Windows Server – Konfigurace auto updatů. Zdroj: vlastní

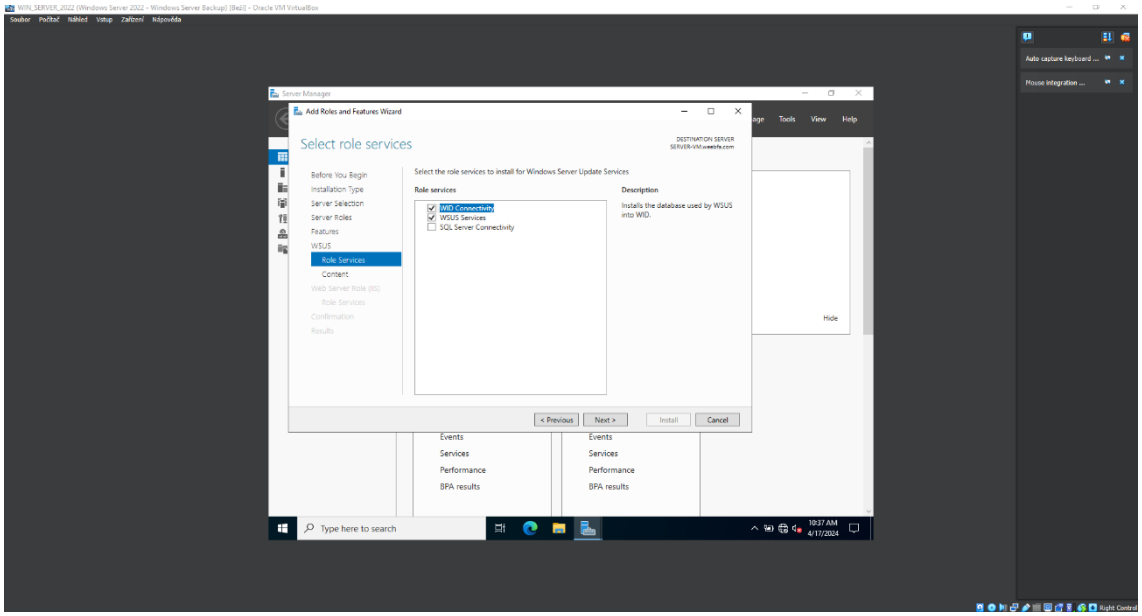
6.7.3.2 Windows klient aktualizace

Konfigurace automatických aktualizací pro Windows klienty nebude stejně snadná jako u Windows Serveru. Na Windows Serveru 2022 je potřeba nainstalovat roli Windows Server Update Services, která umožňuje správcům sítě centrálně nasadit různé aktualizace a záplaty. Instalační proces je totožný jako u DHCP, DNS a Windows Backup. Uživatel si otevře ve Správci serveru průvodce Přidat role a funkce. Nechá vybranou výchozí možnost instalace na základě rolí nebo funkcí. Vybere daný Windows Server. V kategorii Role serveru vybere roli Windows Server Update Services a potvrdí přidání potřebných funkcí k instalaci ve vyskakovacím okně. Obrázek 64 zobrazuje přidání nové role WSUS a přidání potřebných funkcí pro tuto roli.



Obrázek 64 – Windows Server – Přidání role WSUS. Zdroj: vlastní

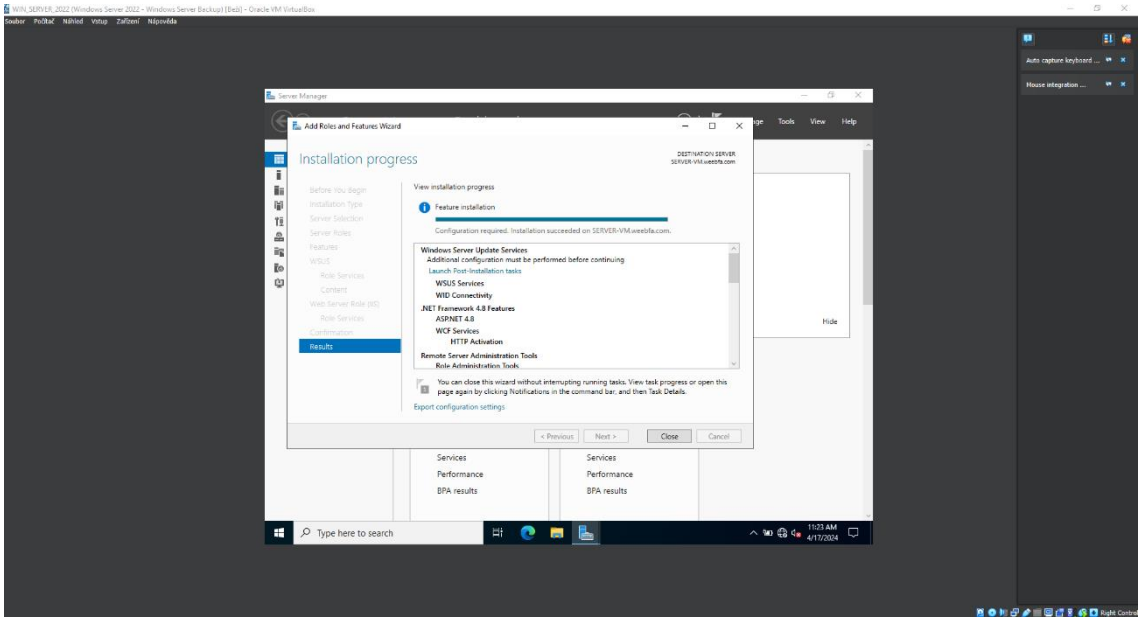
V průvodci Přidání rolí a funkcí se objeví nové okno WSUS s dvěma podokny Role služby a Obsah. V podoknu lze vidět služby, která je potřeba nainstalovat společně s WSUS pro správné fungování. Takže uživatel zde může nechat zaškrtnuté výchozí možnosti WID Connectivity a WSUS Services. Obrázek 65 vizualizuje zaškrtnuté výchozí možnosti Role služby.



Obrázek 65 – Windows Server – WSUS – Role Služby. Zdroj: vlastní

Další podokno se týká obsahu neboli výběru úložiště aktualizací a záplat pro Windows klienty. Už po přečtení informací je zřejmé, že bude nejvhodnější využít samostatný pevný disk. V tomto bodě simulace jsou všechny disky využívané, tudíž je potřeba přidat další pevný virtuální disk pro virtuální stroj ve VirtualBoxu

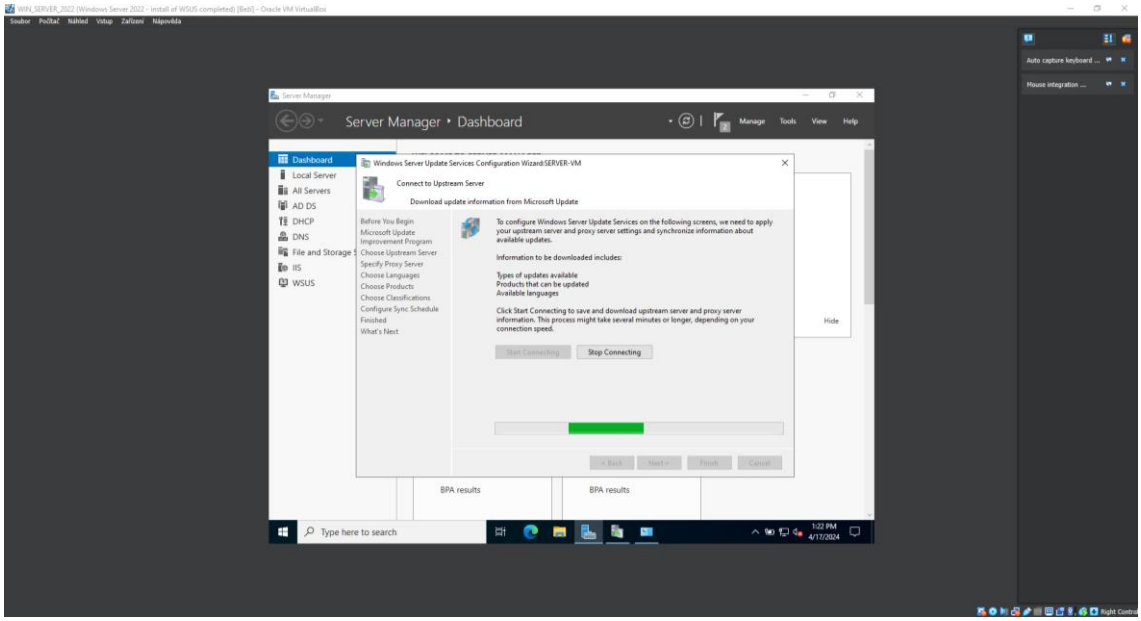
a následně ho naformátovat ve Správě disků. Disk bude mít písmeno U a název Updates. Postup je zcela stejný jako u Zálohování dat, kde se taktéž přidával nový disk. Po přidání nového pevného disku se lze vrátit k podoknu Obsahu a napsat do textového pole cestu disku U:. Poté stačí celého průvodce proklikat tlačítkem Další až k samotné instalaci. Úplné Dokončení instalace může vyžadovat spuštění postinstalačních úloh. Ty lze zapnout na konečném výpisu instalace, kde se objeví hypertextový odkaz Spustit postinstalační úlohy. Po dokončení těchto úloh se hypertextový odkaz změní na normální text, který potvrzuje dokončení postinstalačních úloh v rámci konfigurace. Obrázek 66 prezentuje konečný výpis instalačního procesu s hypertextový odkazem ke spuštění postinstalačních úloh.



Obrázek 66 – Windows Server – WSUS – Postinstalační úlohy. Zdroj: vlastní

Stejně jako u Windows Server Backup služby je potřeba u služby WSUS provést konfiguraci. Uživatel ve Správci serveru v Nástrojích najde položku Windows Server Update Services a tím se mu objeví průvodce konfigurací Windows Server Update Services. První informační okno lze přeskočit tlačítkem Další, ovšem na dalším okně ze simulačních důvod je dobré odškrtnout souhlasení se zapojením do programu společnosti Microsoft pro zlepšení aktualizací. Následující okno Vybrání nadřazeného serveru slouží k určení nadřazeného serveru pro synchronizaci aktualizací a záplat. V tom případě byla zvolena výchozí možnost Microsoft Update. Okno Specifikování Proxy serveru je irelevantní, protože Windows Server nevyužívá Proxy server, tudíž ho lze přeskočit. Další okno se týká

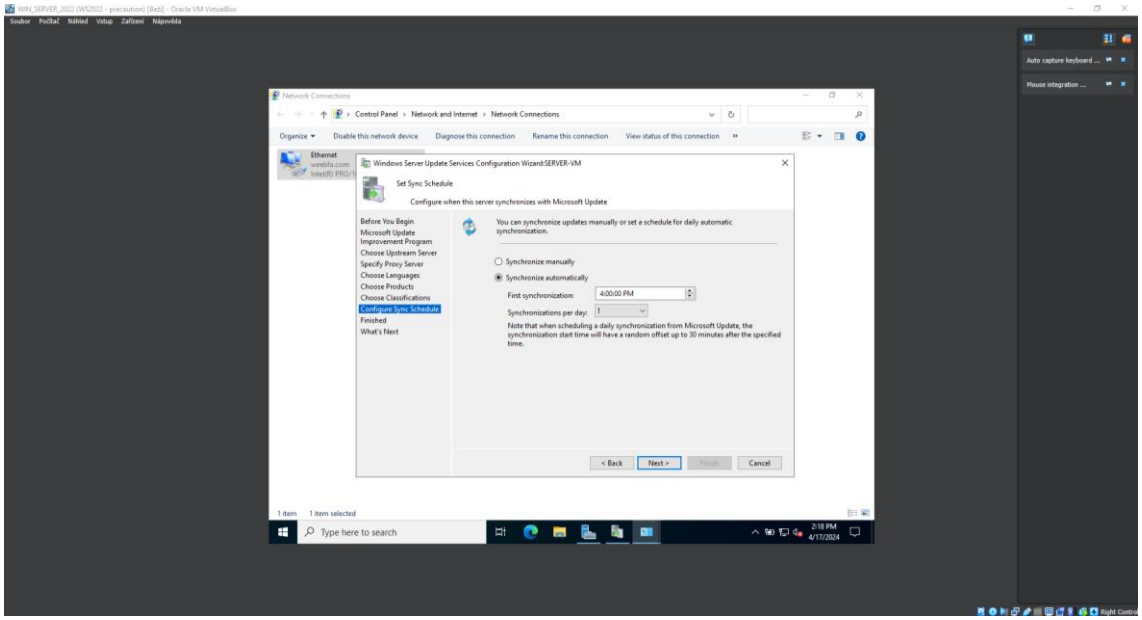
stahování informací ohledně aktualizací a záplat z Microsoft Updatu. Pro tento proces v rámci VirtualBoxu je potřeba přepnout nastavení sítě z Vnitřní sítě na NAT a zároveň nastavit vlastnosti IPv4 pro používaný adaptér na získání automatické IP adresy a DNS serveru. Po přepnutí nastavení sítě lze kliknout na tlačítko Začít se připojovat. Obrázek 67 zobrazuje synchronizační proces za účel získání nejnovější informací ohledně aktualizací a záplat z Microsoft Update.



Obrázek 67 – Windows Server – WSUS – Synchronizace. Zdroj: vlastní

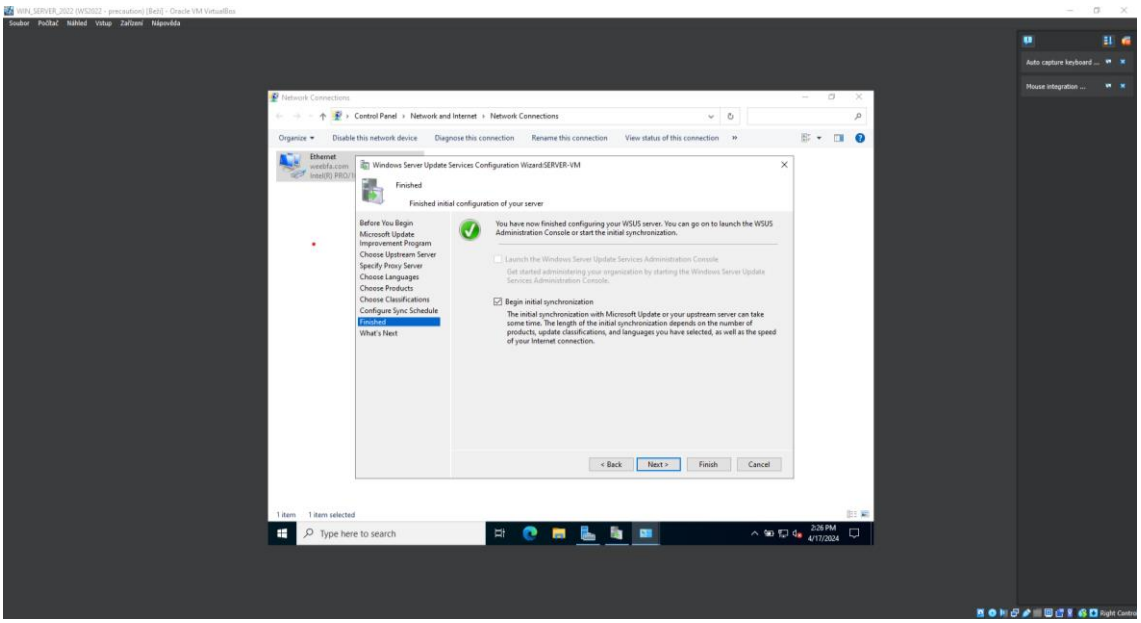
Tento proces může trvat dlouhou dobu. Jakmile bude hotov lze pokračovat na další okno, kde se vybírá jazyk aktualizací a záplat. Po vybrání jazyka uživatele čeká vybrání produktů, které se budou aktualizovat. Nachází se tu všechny produkty společnosti Microsoft, od edicí operačních systému až po konkrétní aplikace. Jako výchozí produkty jsou zde zvoleny všechny edice operačního systému Windows bez rozdílu určení použití. Výběr produktů záleží specifikací společnosti a využívaného hardwaru a software. V rámci simulace byly zvolené používané edice operačního systému Windows. Na dalším okně je určení typu aktualizací, které se mají synchronizovat. Pro účely simulace byly označeny všechny typy. Následující okno se týká nastavení akce synchronizování. Uživatel může ponechat manuální synchronizování nebo může nastavit automatické synchronizování. Parametry automatického synchronizování jsou počet synchronizování během dne a počátek doby první synchronizace. Za účely automatizace hardeningových zásad se zde

uplatnila automatická synchronizace. Obrázek 68 zobrazuje nastavení automatické synchronizace služby WSUS.



Obrázek 68 – Windows Server – WSUS – Auto synchronizace. Zdroj: vlastní

Předposlední okno potvrzuje dokončenou konfiguraci služby WSUS a nabízí spuštění první synchronizace po úspěšné konfiguraci. Tento proces může trvat déle kvůli nastaveným parametrům aktualizací a záplat, jako byly jazyky, produkty a typy aktualizací. Obrázek 69 ukazuje potvrzenou konfiguraci služby WSUS.



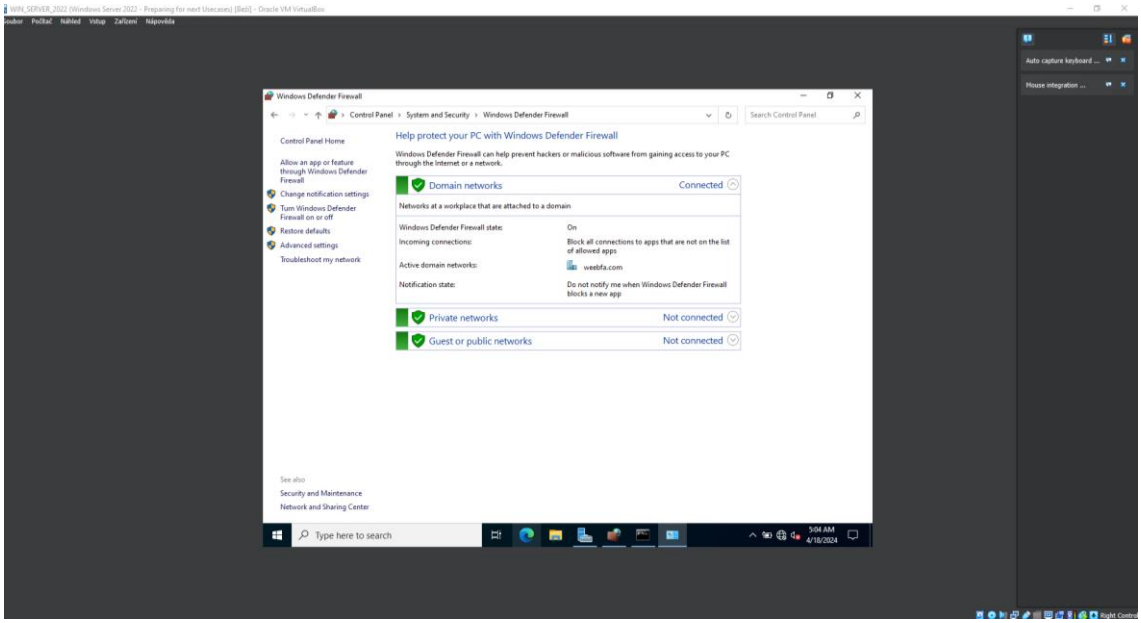
Obrázek 69 – Windows Server – WSUS – Hotová konfigurace. Zdroj: vlastní

Na úplně posledním okně se nacházejí různá doporučení pro ucelení konfigurace služby WSUS, která mohou už být splněna, ale službou WSUS nezaregistrovaná. Pro různé změny nebo doplnění konfigurace stačí otevřít aplikaci

Aktualizace Služeb a konkrétní změny uplatnit zde. V aplikaci je možné spustit stejného průvodce konfigurací a změny udělat v bodech konfigurace. Poslední drobností je zpětné nastavení síťových vlastností pro nadcházející případy užití hardeningu.

6.7.4 Firewall

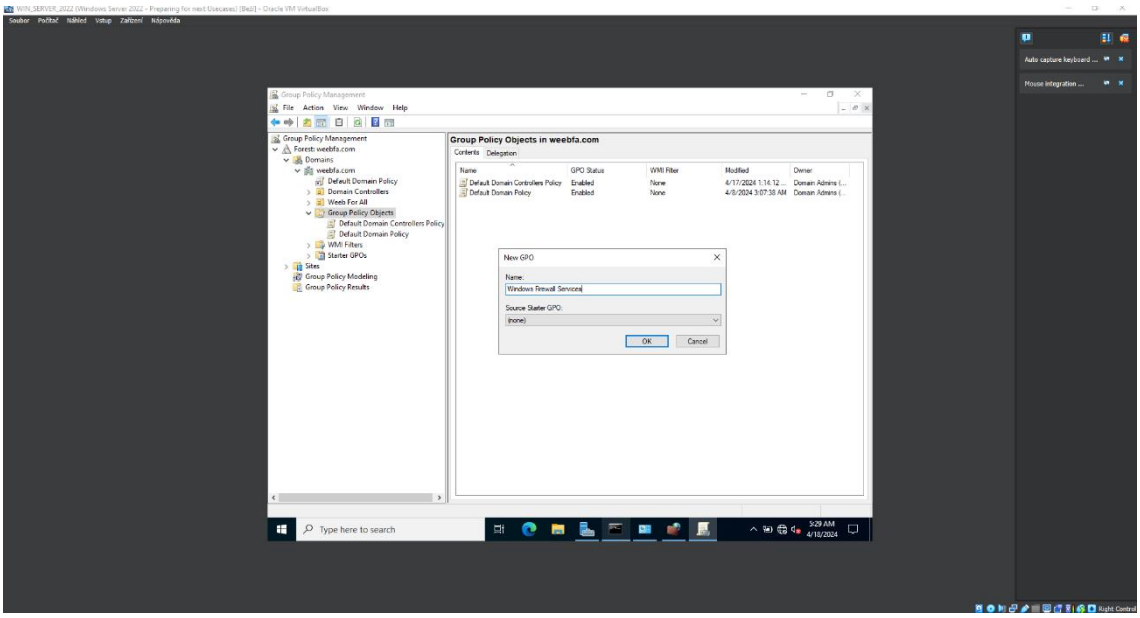
Firewall je nejzákladnější obraná linie proti kybernetickým hrozbám v operačních systémech Windows. Proto je důležité mít Firewall vždy zapnutý. Pro zkontrolování stavu Firewall stačí otevřít Ovládací panely a vyhledat položku Firewall v programu Windows Defender. Pokud tato položka není okamžitě vidět v Ovládacích panelech, nachází se v kategorii Systém a zabezpečení. Nikdy by neměla nastat situace, že Firewall bude vypnutý, neboť hrozí velké nebezpečí napadení operačního systému. Obrázek 70 ukazuje stav Firewallu Windows Serveru.



Obrázek 70 – Windows Server – Stav Firewallu. Zdroj: vlastní

Ovšem může se stát situace při konfiguraci Windows Serveru, že se Firewall přepne do vypnutého stavu nebo bude ho nutné vypnout k otestování spojení s klientskými počítači. Následně uživatel musí zapnout tuto aplikaci a manuálně Firewall opět zapnout. Nastavení a správa Firewallu je velice důležitá a obsáhlá činnost. Firewall umožňuje spravovat různá pravidla, která určují chování operačního systému v dané počítačové síti. Avšak kvůli rozmanitosti těchto pravidel

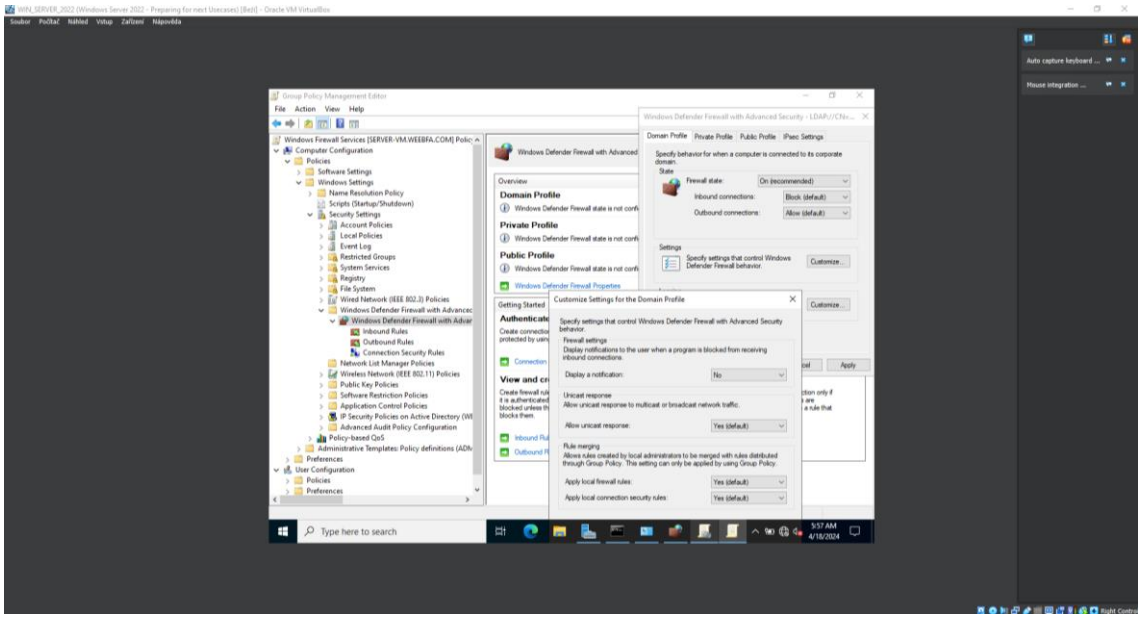
se správa Firewallu může zdát obtížná a repetitivní. Kvůli takovým účelům lze správu Firewallu lehce zautomatizovat pomocí objektů skupinových zásad. Uživatel si otevře aplikaci Správa zásad skupiny, aplikace lze otevřít přes vyhledávací nabídku Windows nebo přes Správce serveru a Nástroje. Zde vyhledá Objekty zásad skupiny, které se nacházejí ve složce Doménová struktura: daná doména -> Domény -> daná doména. Zde stačí označit Objekty zásad skupiny, otevřít kontextovou nabídku a v ní kliknout na položku Nový. Otevře se okno, kde stačí zadat název nového objektu zásad skupiny. Obrázek 71 zobrazuje cestu Objektů zásad skupiny a postup vytvoření nového objektu.



Obrázek 71 – Windows Server – Vytvoření GPO. Zdroj: vlastní

Pro zavedení funkcí danému objektu je potřeba ho označit v levé navigátoru a v jeho kontextové nabídce kliknout na Upravit. Tím se otevře okno editoru, ve kterém lze nastavit potřebné vlastnosti. Pro nastavení Firewallu v rámci objektu zásad skupiny je potřeba vyhledat položku Firewall v programu Windows Defender s pokročilým zabezpečením. Tato položka se nachází v kategorii Konfigurace počítače -> Nastavení systému Windows -> Nastavení zabezpečení -> Firewall v programu Windows Defender s pokročilým zabezpečením. Zde lze vidět, že Firewall je v nenakonfigurovaném stavu. To znamená, že lokálně Firewall je nastavený, ale v rámci objektu skupinových zásad není nakonfigurovaný. Tudíž v tuto chvíli kdokoliv přihlášený na Windows Serveru může změnit nastavení Firewallu. Pro konfiguraci Firewallu v daném objektu zásad skupiny stačí kliknout

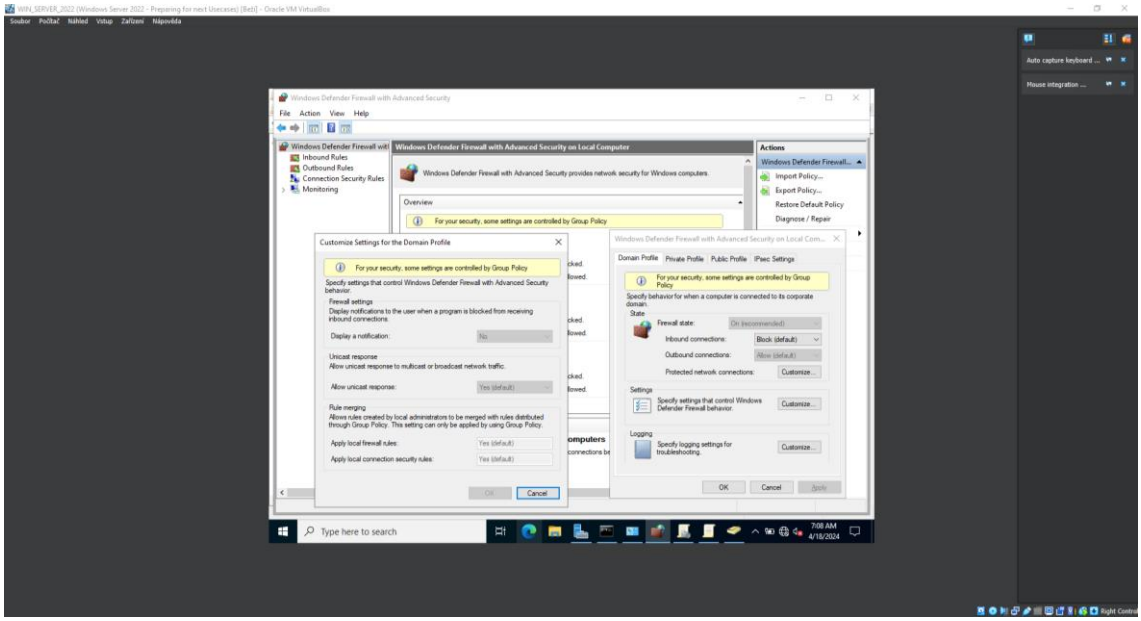
na hypertextový odkaz Vlastnosti brány Firewall v programu Windows Defender. Nyní lze pro každý profil specifikovat nastavení brány Firewall. Je doporučené zvolit veškeré nastavení v sekci Stav na doporučené nebo výchozí hodnoty pro všechny profily. V sekci nastavení je tlačítko Přizpůsobit, které otevře rozšířené nastavení brány Firewall. Hodnota pro Zobrazovat nastavení může být nastavena na Ne a ostatní hodnoty je lepší nastavit na výchozí hodnoty. V sekci Sloučení pravidel je důležité si dát pozor na nastavení těchto hodnot. Výchozí hodnoty zajišťují, že jakékoliv pravidlo vytvořené v rámci objektu zásad skupiny a již nasazené pravidlo ve Firewallu se sloučí. Pokud hodnoty u sloučení pravidel byly nastaveny na hodnotu Ne, tak aby se uplatňovala pravidla pouze z objektu zásad skupiny. V takovém případě by se musel udělat export stávajících pravidel z Firewall a ty pak naimportovat do pravidel Firewallu v objektu zásad skupiny. Obrázek 72 vizualizuje cestu k nastavení brány Firewall pro objektu zásad skupiny.



Obrázek 72 – Windows Server – GPO – Firewall. Zdroj: vlastní

Po kompletní konfiguraci Firewallu a samotného objektu skupiny zásad je důležité objekt přidělit dané organizační jednotce. Jelikož tento objekt se vztahuje na servery v dané doméně, lze ho jednoduchým přetažením umístit do organizační jednotky pro servery. Nicméně tento objekt zásady skupiny se pro aktuální Windows Server neuplatní, protože daný Windows Server je doménovým řadičem a umístěn pod organizační jednotkou Domain Controllers. Aby objekt zásad skupiny byl uplatněn i pro doménové řadiče je potřeba ho přetáhnout i do této organizační

jednotky. Následně lze napsat do příkazové řádky gpupdate /force. Tímto příkazem se zaktualizují zásady skupiny aktivního Windows Server a není potřeba se odhlašovat a opět přihlašovat pro zavedení zásad skupiny. Nyní v aplikaci Firewall v programu Windows Defender s pokročilým zabezpečením lze si všimnout přehledové zprávy, která oznamuje, že některá nastavení jsou z hlediska bezpečnosti řízena zásadami skupiny. Tudíž i když přihlášený uživatel má práva lokálního správce nemůže změnit nastavení Firewall v této aplikaci, jelikož jsou uplatněna z objektu zásad skupiny. Obrázek 73 představuje nasazený objekt zásad skupiny, který řídí nastavení Firewallu.



Obrázek 73 – Windows Server – GPO – Firewall restrikce. Zdroj: vlastní

Po spravovaném Firewallu objektem skupiny zásad je vhodné otestovat příkaz ping v příkazové řádce. Příkaz ping má hlavní vstupní parametr a tím je IP adresa cílového zařízení. V této fázi je možné, že příkaz ping nebude fungovat ze serveru na klienta nebo naopak. Příčin nefunkčního příkazu může být několik. Je vhodné ověřit nastavení Možnosti sídlení, jak na serveru, tak i na klientu. Jelikož byla vytvořená doména, ve které se nachází Windows Server i Windows klientu, přibyla nová kategorie Doména v Možnostech sdílení. Tudíž je nutné zapnout zjišťování sítě i sdílení souborů a tiskáren. Pokud toto nastavení nezprovoznilo příkaz ping je vhodné povolit veškerá pravidla v Inbound Rules tykající se ICMPv4. Tyto pravidla se povolují v aplikaci Firewall v programu Windows Defender s pokročilým zabezpečením. Případně pokud uživatel nechce hledat všechna pravidla tykající se

ICMPv4 může vytvořit nové pravidlo, ve kterém povolí všechny služby využívající ICMP.

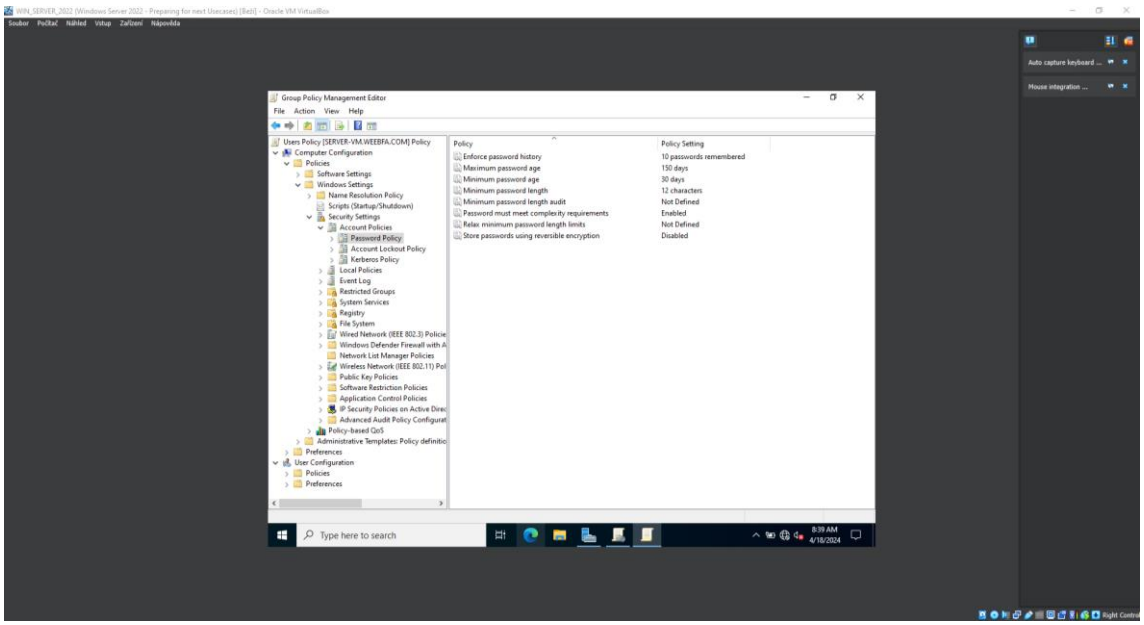
6.7.5 Zásady používaní hesel

Heslo je prvním aspektem zabezpečení čehokoliv. Je velice důležité problematice hesel porozumět a správně aplikovat. Prolomení hesla je nejběžnějším typem kybernetického útoku. Právě proto by hesla mě být koordinována danými zásadami, které specifikují různé vlastnosti hesla. Pomocí objektu zásad skupiny lze tyto vlastnosti nastavit a uplatňovat v dané doméně. Pro běžné uživatele lze vytvořit nový objekt zásad skupiny. V aplikaci Správa zásad skupiny a v položce Objekty zásad skupiny uživatel vytvoří nový objekt, stejně jako u předešlého případu užití Firewallu. Kontextová položka Upravit nového objektu zásad skupiny otevře okno editoru daného objektu. Zde je potřeba vyhledat položku Zásady hesla, která je umístěná v kategorii Konfigurace počítače -> Nastavení systému Windows -> Nastavení zabezpečení -> Zásady účtů. Zde je několik vlastností upravující požadavky na hesla:

- Heslo musí splňovat požadavky na složitost – je zásadní vlastnost, která vyžaduje, aby se heslo skládalo z několika různých znaků. Mezi tyto znaky patří číslice, speciální znaky, velká a malá písmena. Tato vlastnost musí být povolena.
- Kontrola minimální délky hesla – řeší potenciální dopad zvýšení minimální délky hesla. Tuto vlastnost není třeba povolovat, jelikož v tuto chvíli nemá žádný kladný dopad.
- Maximální stáří hesla – definuji maximálně povolenou dobu platnosti hesla. Záleží na komplexnosti dané infrastruktury, pro simulační účely byla použita hodnota 150 (dní).
- Minimální délka hesla – řídí minimální počet znaků, který je obsažen v heslu. Pro běžného uživatele stačí tuto hodnotu nastavit na 12 (znaků).
- Minimální stáří hesla – určuje minimální dobu platnosti hesla neboli kdy nejdříve lze heslo změnit. Tento parametr může být nastaven na 0.

- Ukládat hesla pomocí reverzibilního šifrování – je velice nebezpečná vlastnost, která ukládá hesla skoro ve formě prostého textu. Rozhodně nepovolovat.
- Uvolnit omezení pro minimální délku – slouží pro zvýšení minimální délky hesla, která je obyčejně maximálně na 14 znaků. Povoluje se v případě nutnosti pro zvýšení minimální délky hesla.
- Vynutit použití historie hesel – je nastavení, které ukládá hesla daných uživatelů a kontroluje, zda nově zadaná hesla nejsou totožná s těmi, co už uživatel někdy zadal. Toto nastavení opět záleží na komplexnosti infrastruktury.

Obrázek 74 vizualizuje nastavení vlastností hesel pro běžné uživatele.

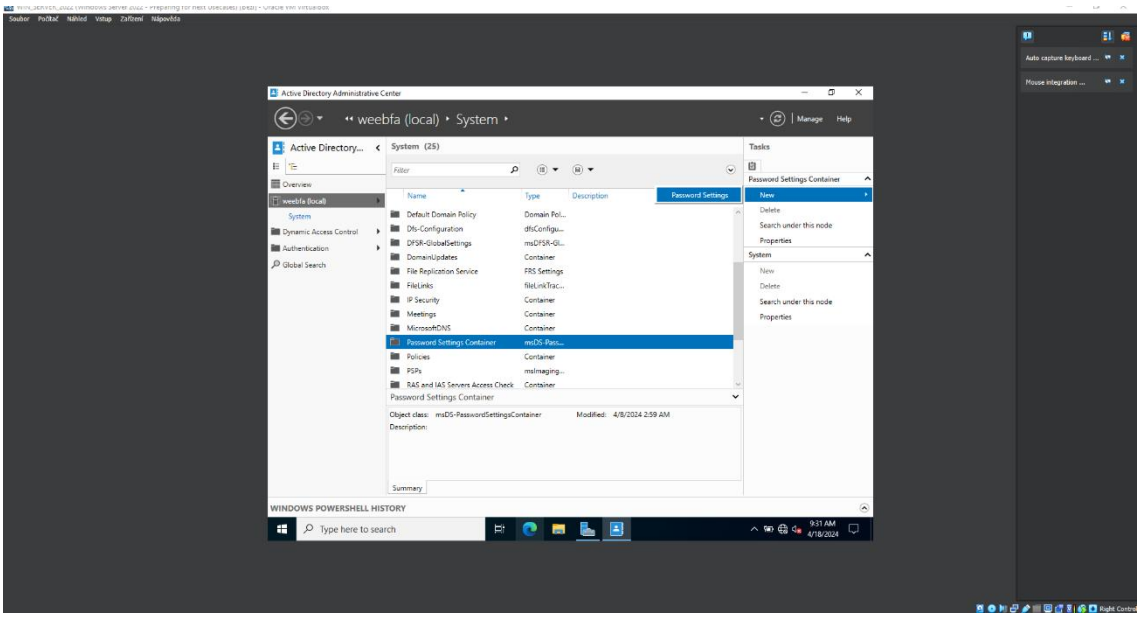


Obrázek 74 – Windows Server – GPO – Uživatelská hesla. Zdroj: vlastní

Nyní lze editor objektu zásad skupiny zavřít a daný objekt přetáhnout do potřebné organizační jednotky Users. Tím jsou zásady používání hesla nastavené pro všechny uživatelské skupiny v organizační jednotce Users a v jejích podjednotkách.

Tímto způsobem lze nastavit zásady používání hesel všeobecně všem uživatelům. Ale pokud by byl požadavek na vytvoření dalších rozdílných zásad používání hesel, doporučuje se využít jemně odstupňované zásady používání hesel. Tudíž využít další objekt zásad skupiny není doporučené. Postup je následující. Uživatel otevře aplikaci Centrum správy služby Active Directory. V ní si označí

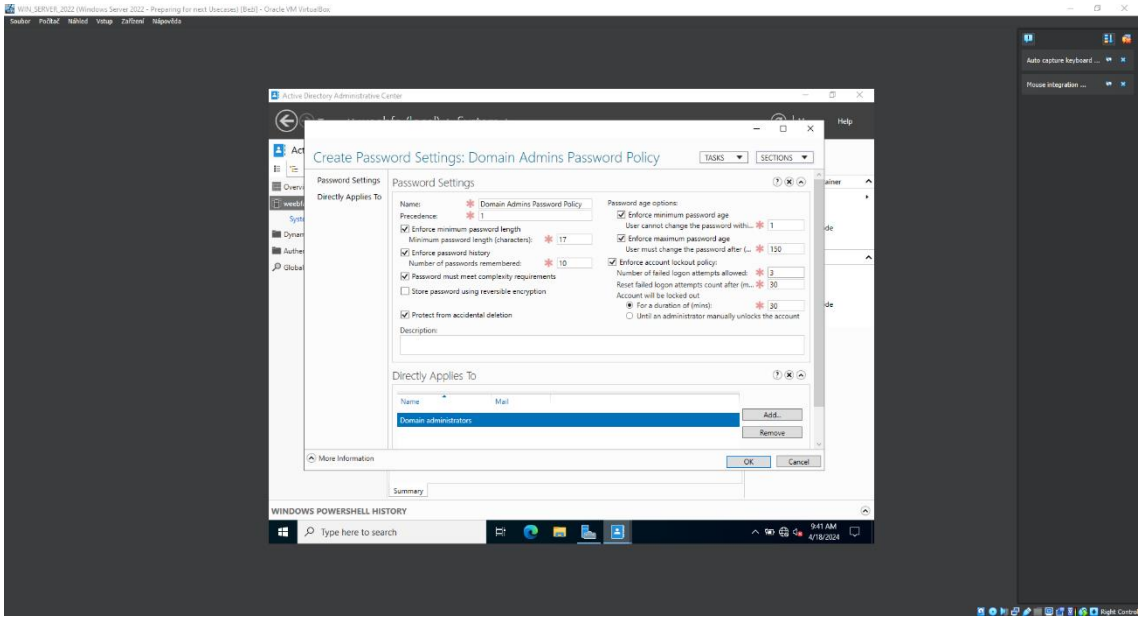
danou doménu (local) a na hlavní panelu uvidí adresářovou strukturu. Je potřeba se dostat do složky System a v ní najít složku Password Settings Container. Tuto složku je potřeba označit a v pravém panelu najet na položku Nový v kategorii Password Settings Container a tím se zobrazí další položka Password Settings, na kterou se klikne. Obrázek 75 prezentuje postup otevření nastavení hesel v aplikaci Centrum správy služby Active Directory.



Obrázek 75 – Windows Server – Kontejner pro nastavení hesel. Zdroj: vlastní

Uživateli se otevře okno Vytvořit nastavení hesla, kde bude nastavovat nové zásady používání hesla pro správce. V tomto okně je pár vlastností navíc oproti objektu zásad skupiny. Název slouží pouze k pojmenování schématu daného hesla. Hodnota přednost vyžaduje číselnou hodnotu, která značí prioritu použití tohoto schéma. Čím nižší hodnota, tím větší priorita. Nachází se tady také políčko s ochranou před náhodným odstraněním, které je vhodné ponechat zaškrtnuté. Poslední vlastnost slouží k nastavení chování při určitém počtu selhaní při zadávání hesla. Nastavuje se zde, kolik selhání je povoleno, doba obnovení pokusů pro přihlášení a na jak dlouho bude účet uzamčen. Poslední nastavení se týká přidělení, komu se toto schéma aplikuje. Uživatel klikne na tlačítko Přidat… a zadá danou skupinu nebo konkrétního uživatele a tlačítkem Kontrola názvu ověří správný název skupiny nebo uživatele. Po nastavení veškerých parametrů lze heslové schéma potvrdit tlačítkem OK a požadavky na heslo se aplikují

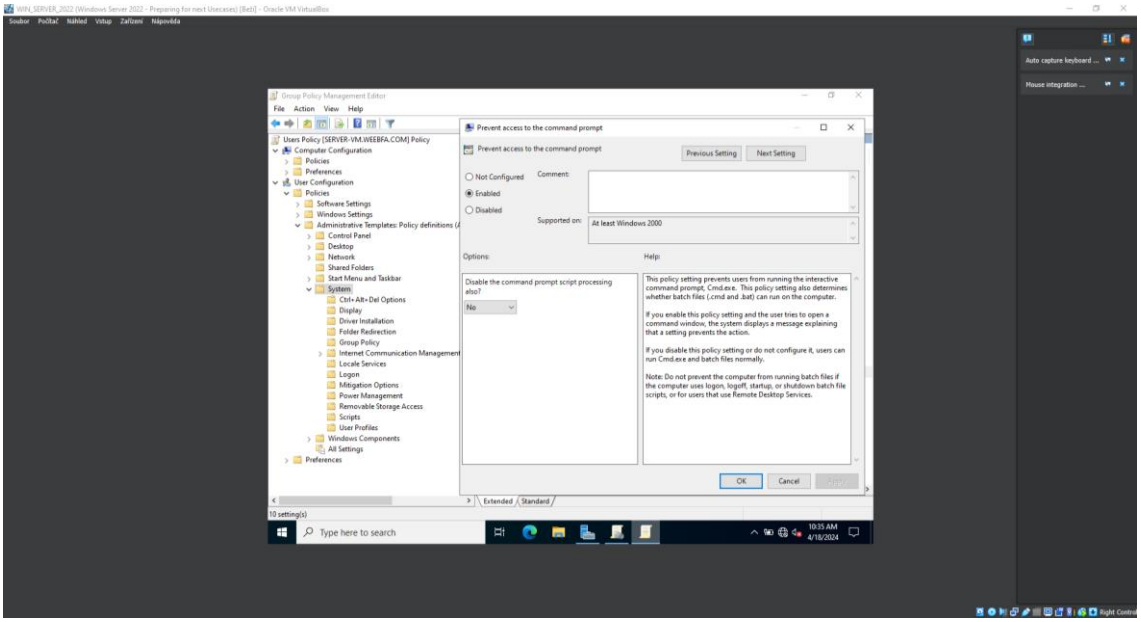
při následující změně hesla. Obrázek 76 zobrazuje nastavení zásady používání hesel pro správce.



Obrázek 76 – Windows Server – Administrátorská hesla. Zdroj: vlastní

6.7.6 Omezení přístupu k příkazové řádce

Příkazová řádka je velice mocný nástroj v operačních systémech Windows. Z bezpečnostního hlediska je vhodné omezit spouštění příkazové řádky pro běžné uživatele a nechat ji dostupnou pro správce nebo potřebné uživatele. Zakázání tohoto nástroje pro běžné uživatele je velice jednoduché. Pro tuto akci je nutné využít objekt zásad skupiny. V aplikaci Správa zásad skupiny v položkách lze upravit stávající objekt nebo vytvořit zcela nový, záleží na požadavcích a specifikací společnosti. V editoru daného objektu je potřeba najít položku Systém, která je umístěná v kategorii Konfigurace uživatele -> Šablony pro správu. V položce systém je samostatná položka Zakázat přistup k příkazovému řádku. Stačí tuto položku povolit a pokud byl vytvořený samostatný objekt zásad skupiny, tak ho přetáhnout do příslušné organizační jednotky. Uplatnění této restrikce se schová následujícím způsobem. Uživatel spustí příkazovou řádku, ovšem pokud ji má zakázanou, tak mu příkazová řádka vypíše, že byla omezena administrátorem. Uživatel může stisknout libovolnou klávesu pro její ukončení, protože do ní nic nenapíše. Obrázek 77 zobrazuje postup pro zakázání příkazové řádky pomocí objektu zásad skupiny.



Obrázek 77 – Windows Server – GPO – Zakázání CMD. Zdroj: vlastní

7 Závěry a doporučení

Hlavním údělem bakalářské práce bylo představit problematiku operačních systémů a reálné zásady nasazení hardeningu.

Teoretická část byla zaměřena na dvě oblasti. První částí bylo představení základních funkcí operačních systémů, různých typů a historie jejich vývoje. Druhou bylo seznámení čtenáře se základními prvky bezpečnosti a jejich využití v operačních systémech. V této části byl kladen důraz na představení bezpečnostních hrozeb, parametrů ochrany a hardeningových pravidel. Tyto části figurovali i jako hlavní cíle teoretické části a byly vysvětleny v následujících kapitolách: Teoretické řešení – Operační systémy; Představení různých OS – Windows, OS X a Linux; Historie OS; Bezpečnost a Bezpečnost v OS.

Praktická část byla zaměřena na vytvoření virtuální firemní infrastruktury a popis skutečných případů užití hardeningu. Virtuální firemní infrastruktura byla postavena na platformě Microsoft Windows Server 2022 a Windows 10 v softwaru pro virtuální stroje VirtualBoxu. Hlavní cíl praktické části byl splněn v kapitole: Hardening. Během simulace vytváření firemní infrastruktury občas docházelo ke kompromisům, kvůli odlišným podmínkám ve virtuálních strojích oproti skutečným operačním systémům. Tyto neshody byly však vyřešeny a porovnány s reálnými případy.

8 Seznam použité literatury

[1] ISBN. MWIINGA, Preston. OPERATING SYSTEM. Researchgate [online]. 2023 [cit. 2023-09-22]. Dostupné z: https://www.researchgate.net/publication/372132620_OPERATING_SYSTEM/link/64a5a0ddc41fb852dd53fc24/download

[2] Desktop Operating System Market Share Worldwide. Statcounter [online]. Dublin, 2023 [cit. 2023-09-04]. Dostupné z: https://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-200901-202309

[3] IGLESIAS, Fernández a Manuel JOSE. Brief Introduction to Operating Systems [online]. 2023 [cit. 2023-09-22]. Dostupné z: https://www.researchgate.net/publication/371274506_Brief_Introduction_to_Operating_Systems doi:10.17605/OSF.IO/38MKS

[4] LINUX RED HAT ENTERPRISE LINUX (RHEL) [7]. Red Hat Enterprise Linux Course Report [online]. International Islamic University Chittagong, 2020, 107 [cit. 2023-09-29]. Dostupné z: doi:10.13140/RG.2.2.33331.66083

[5] Často kladené otázky o Linuxu a GPL. In: Redhat.com [online]. 2021 [cit. 2023-09-29]. Dostupné z: https://www.redhat.com/en/blog/frequently-asked-questions-about-linux-and-gpl

[6] GEEKSFORGEEKS. Evolution of Operating System. Geeksforgeeks.org [online]. 2022, 27.8.2023 [cit. 2023-10-16]. Dostupné z: https://www.geeksforgeeks.org/evolution-of-operating-system

[7] Complete History of the Operating System. History-Computer [online]. 2022, 8.12.2022 [cit. 2023-10-23]. Dostupné z: https://history-computer.com/complete-history-of-the-operating-system

[8] History of Operating System. Scaler.com [online]. 2022, 4.5.2023 [cit. 2023-10-23]. Dostupné z: https://www.scaler.com/topics/history-of-operating-system

[9] Forenzní analýza v OS Windows – video tutoriály [online]. Hradec Králové, 2023 [cit. 2023-10-23]. Dostupné z: https://theses.cz/id/2qs9po/STAG98768.pdf. Bakalářská práce. Univerzita Hradec Králové Fakulta informatiky a managementu Katedra informačních technologií. Vedoucí práce Svoboda Tomáš, Ing. Ph.D.

[10] Essential Computer Science. Online. 1. Apress Berkeley, CA, 2021. ISBN 978-1-4842-7107-0. Dostupné z: https://doi.org/https://doi.org/10.1007/978-1-4842-7107-0. [cit. 2023-12-18].

[11] Nejpoužívanější kryptografické algoritmy. Online, Diplomová práce. Praha: Bankovní institut vysoká škola Praha Katedra informatiky a kvantitativních metod, 2014. Dostupné z: https://is.ambis.cz/th/g5150/Vojtech_Pavel_Diplomova_prace.pdf. [cit. 2023-12-25].

[12] CIA triad (confidentiality, integrity and availability). Online. In: TechTarget. 2023. Dostupné z: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. [cit. 2024-01-22].

[13] The Parkerian Hexad: The CIA Expanded. Online, Diplomová práce. Romeoville: Lewis University Department of Computer & Computer Sciences, 2012. Dostupné z: https://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf. [cit. 2024-01-23].

[14] Security Issues and Challenges in Windows OS Level. Online. Journal of Information Systems & Information Technology (JISIT). 2022, roč. 7, č. 1, s. 19-25. ISSN 2478-0677. Dostupné z: https://www.researchgate.net/publication/367309551_Security_Issues_and_Challenges_in_Windows_OS_Level. [cit. 2024-02-12].

[15] An Overview of Computer Operating Systems and Emerging Trends. Online. Asian Journal of Research in Computer Science. 2023, roč. 16, č. 4, s. 161-177. ISSN 2581-8260. Dostupné z: https://doi.org/10.9734/ajrcos/2023/v16i4380. [cit. 2024-02-12].

[16] Survey on Computer Cyber Security. Online. World of Science: Journal on Modern Research Methodologies. 2023, roč. 2, č. 9, s. 15-26. ISSN 2835-3072. Dostupné z: https://www.researchgate.net/publication/375422309_Survey_on_Computer_Cyber_Security. [cit. 2024-02-16].

[17] Phishing in Web 3.0: Opportunities for the Attackers, Challenges for the Defenders. Online. Advanced Research on Information Systems Security. 2023, roč. 3, č. 2, s. 11-25. Licence: CC BY-NC-ND 4.0. ISSN 2795-4560. Dostupné z: https://doi.org/10.56394/aris2.v3i2.35. [cit. 2024-02-16].

[18] Ransomware. Online. ESET. 2024. Dostupné z: https://www.eset.com/cz/ransomware/. [cit. 2024-02-19].

[19] Increasing the level of network and information security using artificial intelligence. Online. 1. Institute of Research Engineers and Doctors, 2017. ISBN 978-1-63248-131-3. Dostupné z: https://doi.org/10.15224/978-1-63248-131-3-25. [cit. 2024-02-25].

[20] 6 Ransomware Protection Strategies You Must Know. Online. Cynet. 2024. Dostupné z: https://www.cynet.com/ransomware/6-ransomware-protection-strategies-you-must-know/. [cit. 2024-02-25].

[21] Antivirus. Online. ESET. 2024. Dostupné z: https://www.eset.com/cz/antivirus-software/. [cit. 2024-03-13].

[22] Group Policy Object (GPO). Online. In: TechTarget. 2019. Dostupné z: https://www.techtarget.com/searchwindowsserver/definition/Group-Policy-Object. [cit. 2024-03-02].

[23] Group Policy Objects (GPOs): How They Work & Configuration Steps. Online. In: Varonis. 2023. Dostupné z: https://www.varonis.com/blog/group-policy-objects. [cit. 2024-03-02].

9 Přílohy

1)

Příloha č. 1

Zadání bakalářské práce

Autor:	**Vladislav Ivančo**
Studium:	I2100210
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Hardening operačních systémů**
Název bakalářské práce AJ:	Operating systems hardening

Cíl, metody, literatura, předpoklady:

Cílem bakalářské práce je podrobně představit problematiku hardeningu operačních systémů pro zajištění jejich bezpečnosti. V teoretické části budou podrobně představeny operační systémy, principy a techniky hardeningu pro zajištění parametrů důvěrnosti, dostupnosti a integrity dat v operačních systémech. V praktické části budou představeny use-case řešení hardeningu v operačních systémech a podrobně popsány konfigurace tohoto hardeningu.

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	Ing. Tomáš Svoboda, Ph.D.
Datum zadání závěrečné práce:	15.10.2021