VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

SECURITY HARDENING SYSTÉMU WINDOWS SERVER 2016

SECURITY HARDENING OF WINDOWS SERVER 2016

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Hana Křiváková

AUTHOR

VEDOUCÍ PRÁCE — Ing. Viktor Ondrák, Ph.D.

SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Studentka:	**Hana Křiváková**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Security hardening systému Windows Server 2016

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je navrhnout bezpečnostní nastavení Windows Serveru 2016 v konkrétním prostředí.

Základní literární prameny:

DESMOND, Brian, Joe RICBARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. Active Directory. 5th edition. Sebastopol: O'Reilly Media, 2013. ISBN 978-1-449-32002-7.

MOSKOWITZ, Jeremy. Group policy: fundamentals, security, and the managed desktop. 2nd ed. Indianapolis, Ind.: John Wiley and Sons, 2013. ISBN 978-1-119-03558-9.

ROUNTREE, Derrick. Security for Microsoft Windows system administrators: introduction to key information security concepts. Boston: Syngress, 2011. ISBN 978-1-597-49594-8.

ROUNTREE, Derrick a Richard HICKS. Windows 2012 server network security: securing your windows network systems and infrastructure. Amsterdam: Elsevier, 2013. ISBN 978-1-597-49958-3.

STANEK, William R. Active Directory: kapesní rádce administrátora. 1. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2555-7.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2016/17

V Brně dne 28.2.2017

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato bakalářská práce se zabývá problematikou zvyšování bezpečnosti systémů Windows pro servery, konkrétně je teorie aplikována na prostředí Windows Server 2016. Popisuje jednotlivé kroky zvyšování zabezpečení sítě za použití tohoto operačního systému u nejmenované nadnárodní společnosti.

Abstract

This bachelor thesis is focused on the security hardening of Windows systems for servers. In this thesis, the theory is applied on Windows Server 2016 operating system. There are described individual steps one should take to increase network security. The entire project is set in the environment of unnamed multinational company.

Klíčové slova

bezpečnost, zvyšování bezpečnosti, Windows Server 2016, CIS, benchmark, CIS-CAT, řadič domén, členský server, řízení aplikace politik

Key words

security, security hardening, Windows Server 2016, CIS, benchmark, CIS-CAT, Domain Controller, Member Server, Group Policy Management

Bibliografická citace

KŘIVÁKOVÁ, H. *Security hardening systému Windows Server 2016*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 78 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31. května 2017

.....

podpis studenta

Poděkování

Na tomto místě bych chtěla poděkovat vedoucímu bakalářské práce Ing. Viktoru Ondrákovi, Ph.D. za pomoc a rady při práci.

Také bych ráda poděkovala společnosti XYZ, spol. s.r.o. a vybraným zaměstnancům za poskytnutí veškerých materiálů nutných pro zpracování práce, konzultace, ochotu a pomoc.

OBSAH

ÚVOD

Tato bakalářská práce vznikla jako podklad pro nastavení bezpečnostních pravidel pro operační systém Windows Server 2016. Tato pravidla a nastavení byla navržena pro prostředí společnosti XYZ, spol. s.r.o. a její zákazníky, měla by ovšem být použitelná v jakémkoliv podobném prostředí za předpokladu, že jsou provedeny potřebné změny.

Vzhledem k tomu, že se v práci zabývám bezpečností sítě a relativně citlivými informacemi, rozhodla jsem se společnost nejmenovat. V práci budu uvádět název firmy jako XYZ, spol. s.r.o.

Společnost XYZ, spol. s.r.o. se zabývá IT službami a poradenstvím. Operační systémy Windows Server už dlouho využívá jak k interním potřebám organizace, tak jako součást návrhů komplexních informačních systémů pro své klienty – ať už na fyzických či virtuálních serverech. Security hardening je tedy při zavádění nové verze Windows Server naprosto klíčový.

1 CÍL A METODIKA PRÁCE

Cílem této práce je zpracování řešení zabezpečení nové verze operačního systému (OS) pro serverové prostředí, konkrétně Windows Server 2016. Návrh je zpracováván na základě bezpečnostních pravidel a vnitřních politik společnosti XYZ, spol. s.r.o.

Jelikož je bezpečnost velice rozsáhlé téma, zaměřím se pouze na jednu oblast, a to z hlediska softwaru na bezpečné nastavení doménových politik pro Windows Server 2016 ve mnou zvoleném prostředí.

Hlavním podkladem bude srovnání poskytnuté organizací CIS (Center for Internet Security), podle něhož budeme přebudovávat bezpečnostní politiky nového OS. Součástí tohoto procesu bude také průběžná analýza a testování bezpečnosti a funkčnosti systému. Na závěr bude zřízeno testovací prostředí, kde bude ověřena kompatibilita této nové verze OS s implementovaným security hardeningem.

Teoretické informace pro tuto práci budu čerpat z odborných informačních zdrojů a literatury. Také využiji odborných rad zaměstnanců společnosti XYZ, spol. s.r.o.

Výsledkem mé práce by mělo být vhodně navržené řešení, které by společnosti XYZ, spol. s.r.o. umožnilo zavést systém Windows Server 2016 do standardního provozu, a to bez bezpečnostních rizik a bez výrazných omezení pro uživatele.

2 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole se budu věnovat problematice security hardeningu, jeho významu a uplatnění. Dále věnuji zmínku organizaci CIS, čím se zabývá, jejími členy a využití jimi vypracovaných benchmarků v této práci. Také se budu zabývat operačním systémem Windows Server, konkrétně verzemi 2008 R2, 2012, 2012 R2 a 2016.

2.1 Bezpečnost informačních sítí

V této kapitole se budu zabývat základními pojmy z oblasti informační bezpečnosti a pokusím se také nastínit problematiku bezpečnosti vs. dostupnosti.

2.1.1 Základní pojmy

Informační aktiva jsou souhrn aplikací, technologií, dat a osob (15). Za primární aktiva označujeme nejčastěji informace, informační systémy nebo komunikační systém kritické informační infrastruktury. Technologie, zaměstnanci, dodavatelé apod. jsou podpůrná aktiva (16).

Aktiva můžeme charakterizovat také na základě jejich hodnoty – kritériem je cena, kritičnost aktiva nebo obojí. Dále u aktiv hodnotíme zranitelnost neboli citlivost aktiva na působení hrozby. Rozumným přístupem je při definování bezpečnostních politik počítat u každého aktiva s existencí nějakého zranitelného nebo slabého místa (15).

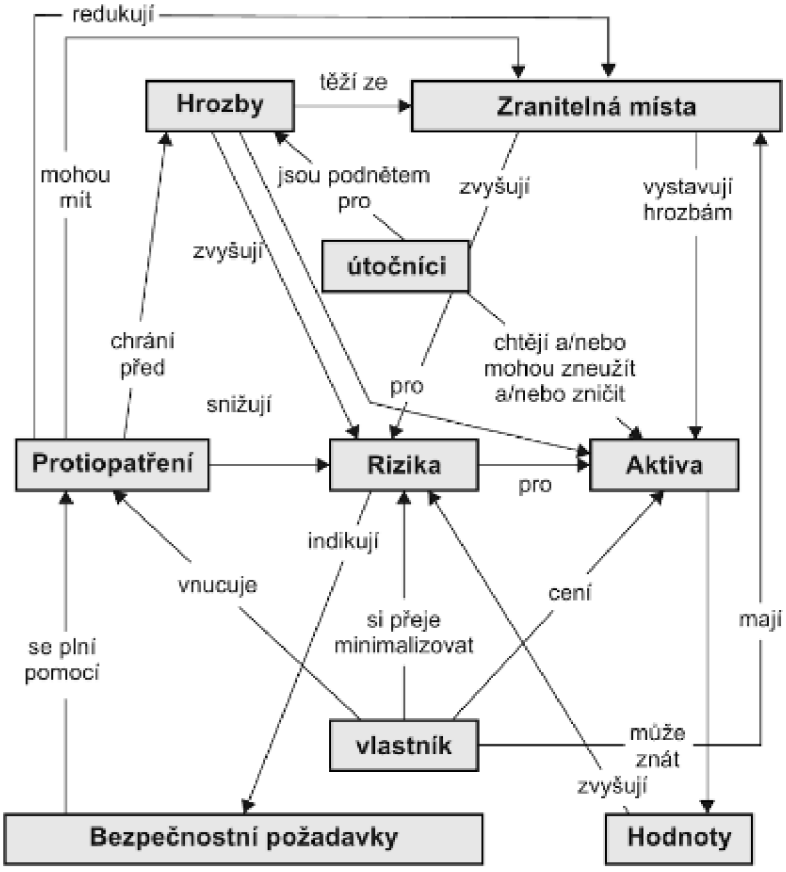
Zranitelnost může být:

- Fyzická – prvek IS je umístěn v lokaci, kde může být poškozen nebo zničen.
- Přírodní – prvek IS je vystaven přírodním vlivům, se kterými nemá šanci se vypořádat (požár, potopa, ...).
- Technologická – konstrukce prvku IS omezuje jeho využití.
- Fyzikální – prvek IS pracuje na fyzikálních principech, které umožňují jeho zneužití.
- Lidská – neznalost a omyly lidí (15).

Hrozbou nazýváme vnější nebo vnitřní vliv, působící na aktivum, který může způsobit nežádoucí změny ve struktuře, vlastnostech a vazbách aktiva. Pokud tyto změny ohrozí bezpečnost IS, mluvíme dále o bezpečnostní hrozbě (17).

Pokud bezpečnostní hrozba způsobí změnu na daném aktivu mluvíme dále o bezpečnostní události. Je-li touto bezpečnostní událostí ohrožen informační systém, používáme termín bezpečnostní incident (17).

Jako riziko označujeme pravděpodobnost, že hrozba využije zranitelnosti IS a způsobí poškození aktiva. Úroveň rizika charakterizuje nebezpečnost hrozby pro organizaci (16, 17).



Obr. 1: Základní pojmy spojené s bezpečností a vztahy mezi nimi (15)

2.1.2 Bezpečnost a dostupnost

Abychom úspěšně ochránili integritu systému, zajistili utajení citlivých dat nebo zabránili vstupu nežádoucí osoby, musíme systém zabezpečit. Bezpečnostní pravidla ale ne vždy korespondují s požadavky uživatelů na dostupnost dat (5).

Základními kameny každé bezpečnostní politiky jsou soukromí, důvěra, autenticita a integrita. Správce systému musí tedy být schopný udržet určité informace tajné, potřebuje vědět komu může udělit k těmto datům přístup a tito uživatelé musí mít způsob, jak prokázat systému svou identitu. Nezbytný je také proces dokazování, že systém nebyl kompromitovaný (5).

Na druhou stranu je třeba se přesvědčit, že uživatelé mají přístup k datům, která potřebují ke své práci. Administrátor tedy přiděluje přístupy, uděluje výjimky, otevírá porty atd., vše proto, aby uživatelé měli co možná nejrychlejší a nejsnadnější přístup k datům. Tím ovšem oslabuje bezpečnost systému (5).

Ideální míra dostupnosti při zachování co možná nejvyššího zabezpečení je základním problémem při security hardeningu – budu se jím tedy zabývat v průběhu celé této práce (5).

2.2 Vymezení Security Hardeningu

Jelikož je téma bezpečnosti a security hardeningu velmi rozsáhlé, zaměřím se ve své práci na užší okruh, a to vydefinování korektních doménových politik vhodných pro bezpečný systém.

Počítačová bezpečnost se poslední dobou objevuje ve zprávách čím dál častěji. Ať už úspěšné či ne, útoky na počítačové sítě, od malých podniků až po nadnárodní korporace, jsou na denním pořádku. Pokusy infiltrovat síť přímo jsou ale pouze jednou z hrozeb, které musí administrátoři čelit. Další značný bezpečnostní problém představují například viry, červy nebo trojské koně. Nesmíme ale zapomenout ani na lidský faktor.

Zaměstnanec, který není poučen o tom, jak se má na interní síti chovat, často způsobí víc škody než užitku (1).

Tím vším se zabývá security hardening, tedy způsoby a metodami, jak se obrnit vůči nepřátelskému prostředí internetu. „*Je to proces ochrany systému před neznámými hrozbami.*“ (1, s. 2)

2.2.1 Centrum pro internetovou bezpečnost

Centrum pro internetovou bezpečnost (CIS, Center for Internet Security) je nezisková organizace založena v roce 2000 za účelem vylepšení bezpečnosti na síti. Hlavním cílem je vývoj, hodnocení a propagace osvědčených postupů v oblasti kyberbezpečnosti (3).

Členy CISu se mohou stát jak vládní organizace a soukromé firmy, tak i jednotlivci. Členové se seskupují do komunit podle zaměření a společně sestavují bezpečnostní benchmarky (Security Benchmarks), které poté slouží jako celosvětové standardy pro internetovou bezpečnost (3).

Další cíle CISu jsou například pomoc při sdílení informací mezi veřejným a soukromým sektorem, monitorování sítě 24 hodin denně 7 dní v týdnu, včasná varování před kyber hrozbami, identifikace a zmírnění dopadu zranitelností a reakce na útoky (3).

2.2.2 Bezpečnostní benchmarky

Oddělení zabývající se bezpečnostními benchmarky stanovuje globální standardy pro internetovou bezpečnost. Každý člen CISu se může přidat ke kterékoliv komunitě, čímž je zajištěna rozmanitost odborných názorů. Dokumenty jsou sestavovány na základě společné shody členů komunity (v případě této práce to byl CIS Microsoft Windows Benchmark) (3).

Pomocí benchmarků CIS společnostem poskytuje dobře definovaný, nezaujatý způsob, jak ohodnotit informační systém a vylepšit jeho zabezpečení. K dispozici je na webových

stránkách rozsáhlá dokumentace k jednotlivým systémům, zdarma programy hodnotící stav vašeho systému, certifikace a diskuze na nespočet témat (3).

K dispozici je program CIS-CAT, který po instalaci oskenuje zvolený systém (ať už Windows nebo kterýkoliv jiný vybraný) a automaticky porovná výsledky s bezpečnostním benchmarkem. Poté vypíše seznam míst, ve kterých se analýza s benchmarkem neshoduje. Už je jen na správci systému, zda nalezené nesrovnalosti jsou přijatelné bezpečnostní riziko nezbytné pro bezproblémový chod společnosti, nebo je třeba je řešit (7).

2.3 Windows Server

Windows Server je souhrnný název pro skupinu operačních systému určených pro provoz serverů. Tato skupina zahrnuje produkty od verze Windows Server 2003 nahoru. Prvním OS pro využití na serverech byl Windows NT 3.1 následován NT 3.5, NT 4.0 a Windows 2000 Server – první serverový OS obsahující Active Directory, DNS Server, DHCP Server a Group Policy (6).

2.3.1 Popis jednotlivých verzí

Windows Server 2008 byl 8. produktem v serverové řadě Microsoftu. Oproti předchozím verzím poskytoval Server 2008 Active Directory role s identitou, možnost certifikace, služby pro spravování práv, Failover Clustering, self-healing NTFS, a Hyper-V. Přidáním Hyper-V dal Microsoft jasně najevo svůj úmysl zaměřit se v příštích letech na virtualizaci (4).

Rok poté vydal Microsoft Windows Server 2008 R2. Navzdory podobnému jménu se tato verze výrazně liší od předchozí. Je postavena na jádru Windows 7, zatímco Server 2008 byl postaven na Vistách. Server 2008 R2 se ještě více soustředí na virtualizaci a v této oblasti jsou v něm provedena podstatná vylepšení. Dále obsahuje nové IIS (7.5), PowerShell 2.0. Bylo vydáno 8 modifikací (mezi nimi například Standard, Enterprise, Datacenter ...) (4).

Verze 2008 R2 byla nahrazena Windows Server 2012, který byl vyvíjen současně s Windows 8 a na stejném designu. Obsahovala nový Server Manager, IIS 8, novou verzi Hyper-V, možnost zálohování v Cloudu, nový systém správy souborů. Oproti 2008 R2, byly ale vydány pouze 4 modifikace (Foundation, Essentials, Standard, Datacenter) (4).

V roce 2013 přišel Microsoft s Windows Server 2012 R2. Jako u všech předchozích serverových systému byl i 2012 R2 postaven na souběžně vyvíjeném jádru pro stolní počítače – v tomto případě tedy Windows 8.1. Podstatné změny zahrnovaly PowerShell v4, integraci MS Office 365, IIS 8.5, antivirový program Defender, opět vylepšení v oblasti virtualizace, zlepšení Group Policy. Stejně jako jeho předchůdce vyšel Server 2012 R2 ve čtyřech modifikacích (4).

Nejnovější verze Windows Serveru vyšla koncem roku 2016. Je opět postavena na jádru Windows pro stolní počítače a laptopy – Windows 10. Zaměřuje se na virtualizaci a práci s Cloudem. Pro virtualizaci aplikací je zavedena nová role Windows Containers, dále také MultiPoint Services, IIS 10, PowerShell v5. Mnoho změn bylo provedeno také pro Hyper-V. Microsoft navíc změnil i způsob licencování (4).

2.3.2 Srovnání jednotlivých verzí

Srovnání jednotlivých verzí není jednoduché. Nelze říct, že jedna verze je lepší než druhá. Postupem času se sice vylepšovala bezpečnost, ale pouze v reakci na množící se hrozby. Obecně je rozumné používat nejnovější verze operačních systémů, jelikož je jim ze strany výrobce věnována nejvyšší pozornost – vychází častěji aktualizace, pokrývají nejnovější hrozby a jsou kompatibilní s aktuálními verzemi nejrůznějších programů (4).

Tab. 1: Porovnání verzí systému Windows Server (6).

Jméno	Datum vydání	Jádro	Typ OS
Windows Server 2003	24.4.2003	NT 5.2	Server, Síťová zařízení, vestavěné systémy, HPC
Windows Server 2008	27.2.2008	NT 6.0	Server
Windows Server 2008 R2	22.10.2009	NT 6.1	Server
Windows Server 2012	4.9.2012	NT 6.2	Server
Windows Server 2012 R2	18.10.2013	NT 6.3	Server
Windows Server 2016	2016	NT 10.0	Server

2.4 Active Directory

Systém Windows Server obsahuje adresářovou službu Active Directory už od verze Windows 2000. Adresářová služba ukládá informace potřebné k použití a správě distribuovaných prostředků v adresáři (12).

Domény jsou logickými seskupeními objektů, které sdílí společné databáze služby Active Directory. Domény jsou logicky seskupeny do stromů. Stromy domén jsou dále seskupovány do doménových struktur (12).

Pro logické uspořádání objektů v doméně jsou užívány organizační jednotky (OU). S jejich pomocí lze vytvářet hierarchii v rámci domény (12).

Domény služby Active Directory obsahují centrální úložiště dat snadno dostupné ze všech umístění v síti, za předpokladu korektní autentizace uživatele. Primárním protokolem AD je LDAP – standardní protokol pro adresářové služby, umožňuje tedy vzájemnou spolupráci s jinými adresářovými službami a klienty (12).

Pro uspořádání skupiny do hierarchické struktury využívá AD službu DNS. DNS slouží k překladu snadno čitelných názvů hostitelů na číselné adresy protokolu IP. Je nezbytné, aby byl každému počítači v doméně přidělen plně kvalifikovaný název domény (FQDN) (12).

Domény DNS mají strukturu stromu s jedním kořenem. Tímto kořenem je tzv. kořenová doména, která se zapisuje jako tečka. Pod ní jsou v hierarchii domény nejvyšší úrovně (TLD) – ty jsou buď geografické (pro jednotlivé státy) nebo podle funkce (pro organizace, armádu ...). Dalším stupněm hierarchie jsou nadřazené domény (domény druhého řádu) – ty mohou být dále rozděleny na subdomény neboli podřízené domény (domény třetího řádu; rozdělení v rámci organizace) (13).

Služba Active Directory je na službě DNS závislá, je tedy nutné ji nainstalovat před nebo současně s instalací ADDS (12).

2.4.1 Řadiče domén a členské servery

Jakýkoliv počítač s operačním systémem Windows Server může být nakonfigurován jako samostatný server, členský server nebo řadič domény (12).

Řadič domény je takový počítač, na kterém je uložen adresář služby Active Directory včetně veškeré funkcionality a protokolů (8).

Řadiče domény řídí uživatelské interakce a komunikaci v rámci i mezi doménami. Ověřují pokusy o přihlášení uživatelů, vyhledávají objekty, zajišťují změnu a uchování informací (12).

Kritickou součástí úspěšného a bezpečného zavedení AD je také zabezpečení fyzický serverů na nichž jsou řadiče domén instalovány – to ovšem může být problém, jelikož lokace kanceláří a prostor, kde jsou servery uloženy není vždy ideální. Řešením je řadič domén pouze pro čtení (RODC) – oproti standardním DC, které slouží jak pro čtení, tak pro zápis a jsou umisťovány do zabezpečených lokací (8).

Členský server (member server) je každý server připojený do domény, který nemá funkci řadiče domény. Členský server může být převeden na řadič domén procesem povýšení (promotion) (8).

2.4.2 Skupinové politiky

Skupinové politiky jsou pravidla a předvolby nastavitelné na operačních systémech Windows, které určují chování systému v daných situacích. Lze pomocí nich například nastavit, co uživatelé smí a nesmí dělat, kam mají přístup nebo jak má systém reagovat v určitých podmínkách. Tato nastavení lze slučovat do skupin zvaných Objekty skupinové politiky (GPO) (14).

Každý GPO obsahuje dvě části: Uživatel a Počítač. Tyto části se nazývají nody, říká se jim ale také uživatelská větev a počítačová větev. První level pod uživatelským i počítačovým nodem obsahuje softwarová nastavení, nastavení pro Windows a administrativní šablony. Každý z těchto levelů obsahuje další podsložky (9).

Pro manipulaci s těmito složkami a v nich obsaženými politikami na řadiči domén využíváme Group Policy Management konzoli (9).

2.4.3 Group policy management konzole

Group Policy Management Console (GPMC) je nástroj dostupný jako součást operačních systémů Windows Server. GPMC slouží pro administraci doménových politik. GPMC je dnes součástí každého serverového OS – je součástí při instalaci ADDS, lze jej ale nainstalovat i samostatně jako MMC snap-in (9).

3 ANALÝZA SOUČASNÉHO STAVU

V této kapitole představím společnost a její strukturu, uvedu zastoupení jednotlivých verzí systému Windows Server a také odhad počtu serverů (jak fyzických, tak virtuálních), na které se bude v prvním půlroce instalovat Windows Server 2016.

3.1 Základní údaje o firmě

3.1.1 Historie firmy

Společnost XYZ, s.r.o. byla založena ve Finsku v roce 1968. V prvních letech sloužila jako počítačové centrum. IT systémy byly vyvíjeny převážně pro banky a lesnický průmysl.

Během IT boomu v 90. letech společnost rychle rostla a rozvíjela se; posílila svou pozici v telekomunikačním sektoru.

Počátkem 21. století se společnost rozšířila na zahraniční trhy – nejdříve ze severu do Evropy, pak do Indie a Ameriky. V roce 2007 se firma opět zaměřila na severský trh, telekomunikační služby ovšem nadále rozvíjela globálně.

Postupně se zvyšovala důležitost zahraničních zdrojů a společnost rozšiřovala svou nabídku produktů a služeb, společně s dalšími pobočkami a servisem pro zákazníky. V roce 2012 firma upoutala pozornost B2B světa představením nového Cloud Serveru a spuštěním Cloud Server mirrors – jádra nové technologické strategie, která se soustřeďuje na čtyři hlavní oblasti: cloud, big data, mobilitu a sociální média.

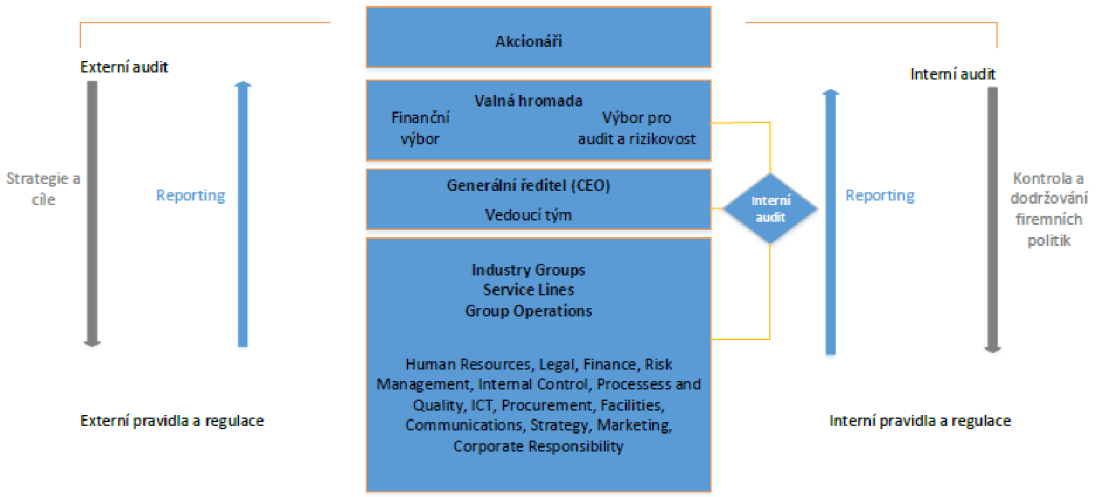
Společnost je také velmi aktivní v oblasti ochrany životního prostředí s jedním z prvních projektů o efektivním využití energie z roku 1978. Projekt se věnoval využití nadbytečného tepla vyprodukovaného data centrem ve Švédsku k vyhřívání přilehlých kanceláří. Dnes je znovu využití energie základním požadavkem pro všechna data centra firmy, z nichž mnohé jsou připojeny k lokálním sítím a poskytují energii pro kanceláře a soukromé objekty.

3.1.2 Předmět podnikání

- Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona,
- poskytování software, poradenství v oblasti informačních technologií, zpracování dat, hostingové a související činnosti a webové portály,
- pronájem a půjčování věcí movitých,
- poradenská a konzultační činnost, zpracování odborných studií a posudků,
- výzkum a vývoj v oblasti přírodních a technických věd nebo společenských věd,
- mimoškolní výchova a vzdělávání, pořádání kurzů, školení, včetně lektorské činnosti,
- poskytování software prodej hotových programů na základě smlouvy s autory nebo vyhotovování programů na zakázku,
- koupě zboží za účelem jeho dalšího prodeje a prodej,
- zpracování dat, služby databank, správa sítí,
- výzkum a vývoj v oblasti informačních a komunikačních technologií (18).

3.1.3 Organizační struktura

Firma je akciová společnost, česká pobočka je ovšem v OR zapsaná jako společnost s ručením omezeným. V čele je generální ředitel (CEO) – ten je jmenován do funkce správní radou. Členové správní rady jsou voleni akcionáři na každoroční valné hromadě.



Obr. 2: Organizační struktura XYZ, spol. s.r.o. (Zdroj: vlastní zpracování)

Na každoroční valné hromadě, která se koná tradičně v srpnu, jsou mimo jiné voleni členové správní rady a auditoři, rozhoduje se o jejich kompenzaci a diskutují se záležitosti jako skupování a výdej akcií.

Správní rada má mezi šesti a dvanácti členy – jsou jmenováni na jeden rok. Cílem společnosti je kromě profesní kompetence členů jejich rozmanitost na základě pohlaví, věku, oboru, profesní minulosti, zkušeností.

Generální ředitel je volen správní radou a je zodpovědný za operativní managment, interní efektivitu operací a kvalitu. Ředitel je v čele Vedoucího týmu, který zahrnuje vedoucího pro odvětví průmyslu, vedoucího servisních linek, ředitele divize financí a vedoucího lidských zdrojů. Členové Vedoucího týmu jsou jmenování do funkce předsedou správní rady na základě návrhu generálního ředitele.

3.1.4 Cílová skupina

Společnost se zaměřuje na střední a velké firmy a veřejné zakázky. Primárním trhem je severní Evropa – tam cílí na zákazníky, kteří mají zájem o komplexní služby respektující ekologickou politiku společnosti. Mezi klienty firmy jsou banky, školy, nemocnice, vládní instituce, ale i množství soukromých firem.

3.2 Prostředí

Při zavádění nového operačního systému je systém nejdříve nainstalován v testovacím a až poté v produkčním prostředí.

3.2.1 Testovací prostředí

Pro testování nového softwaru jsou standardně dedikované testovací servery, kompletně oddělené od produkčního prostředí, aby se předešlo jakékoliv nechtěné komunikaci mezi testovacím a produkčním prostředím.

Servery jsou vybaveny softwarem pro vytváření virtuálních jednotek (VM). Nejčastěji se využívá VMware nebo Hyper-V. Virtuální jednotky jsou organizačně zařazeny do jednoho clusteru – tak je umožněno sdílení zdrojů (například CPU nebo RAM).

Testování se provádí jak pro samostatné (nezávislé), tak pro doménové servery. Po instalaci Active Directory Domain Services (v případě Linuxu Samba PDC) na jednu z virtuálních jednotek se do domény přidá několik member serverů. V případě MS Windows se přidávají další role (DNS, DHCP, web services, Print and File services, ...) a testuje se komunikace mezi řadičem domén a členskými servery – nejčastěji PowerShell Remoting, Remote Desktop Connection, komunikace s BladeLogic Server Automation konzolí.

3.2.2 Produkční prostředí

Po úspěšném vyřešení všech potencionálních problémů v testovací fázi je operační systém nainstalován do produkčního prostředí. Osvědčeným postupem společnosti je naplánovat krátké období, během kterého bude systém využíván pouze interně, aby se doladily poslední detaily a také z důvodu zjištění chování systému ve větším měřítku.

Dalším krokem je začít nabízet produkty založené na novém systému klientům.

3.2.3 Windows Server 2016

Windows Server 2016 je tedy nejdříve zaveden do testovacího prostředí, ve kterém se zjišťuje jeho kompatibilita s nejrůznějším softwarem a aplikacemi (jak třetích stran, tak vyvinuté společností XYZ, spol. s.r.o.), které jsou poskytovány klientům spolu s operačním systémem. Dále se testuje komunikace member serverů s řadičem domén, funkčnost firewallů a antivirových programů, instalují se jednotlivé role, zjišťuje se výkonnost serverů při zátěži atd.

Přestože jsou i testovací servery chráněny firewally a bezpečnostními pravidly, zásadně se nepoužívají reálná data. V testovací fázi se totiž také testují a aplikují bezpečnostní politiky předdefinované organizací CIS. Odstraňují se politiky, u kterých nastane nějaký

konflikt s aplikacemi nebo softwarem, a přidávají se další, které bezpečnostní experti považují za nezbytné. Tato nastavení a úpravy ovšem mohou systém otevřít bezpečnostním hrozbám. Použití reálných dat je tedy nevhodné – provádí se jejich zneplatnění.

3.3 Operační systémy

V současné době společnost využívá jak Linux, tak Windows. Z Unixových OS jsou to Red Hat Enterprise Linux (RHEL) a SUSE Linux Enterprise Server (SLES). Od společnosti Microsoft je využíván produkt Windows Server.

Firma se snaží vždy rychle a kvalitně zavádět nejnovější verze operačních systémů. Momentálně je využíván RHEL verze 6 a 7 a SLES verze 11 a 12, a Windows Server 2008, 2008R2, 2012, 2012R2. Tyto verze jsou používány interně a poskytovány zákazníkům. Nadále jsou udržovány i služby pro Windows Server 2003 – tato verze není již nadále využívána interně, ani na ni nejsou upravovány nové produkty. Je udržován pouze servis pro existující systémy, které WS 2003 využívají.

Koncem roku 2016 začalo testování a implementace Windows Server 2016 pro interní použití. Během roku 2017 bude systém kompletně zaveden do provozu i s dokončenými bezpečnostními politikami. Po předem stanoveném časovém úseku začne firma nabízet produkty a služby postavené na tomto operačním systému.

3.4 Požadavky investora

Původním požadavkem investora v rámci tohoto projektu bylo najít univerzální nastavení politik použitelné napříč všemi používanými verzemi OS Windows Server. Toto se ukázalo jako neproveditelné z důvodu menších či větších rozdílů v architekturách těchto systémů. Byly tedy vydefinovány politiky pro každý OS zvlášť.

Dalším požadavkem bylo snadné nastavení všech politik na serveru. Buď pomocí skriptu, jednoduchého příkazu nebo importu pomocí některého doplňku server manageru.

Bylo také důležité zajistit možnost nahrání politik jak na řadiče domén, kde budou dále poděděny jak na členské servery, tak na stand-alone servery, na nichž není nainstalována GPMC.

Dalším krokem bylo sepsat návody k použití navrženého bezpečnostního řešení a další dokumentaci. K tomu patří také možnost kontroly hodnot nastavených na serveru oproti našemu řešení.

3.5 Shrnutí analýzy současného stavu

Z analýzy současného stavu vyplývá, že jednotné nastavení politik pro serverové operační systémy je pro bezpečnější chod firmy kritický. Pro starší verze OS Windows Server byly politiky navržené jako první, v této práci se tedy věnuji verzi Windows Server z roku 2016.

V první fázi je potřeba nastavení bezpečnostních politik navrhnout s ohledem na software třetích stran používaný v rámci celé firmy. Dále budeme tyto politiky nastavovat v testovacím prostředí a zjistíme jejich funkčnost před tím, něž je zavedeme do produkčního prostředí a začneme nabízet zákazníkům.

Vzhledem k tomu, že Windows Server 2016 je nově zaváděný operační systém, budeme předpokládat, že zpočátku nebude počet serverů s ním vysoký, v porovnání s ostatními verzemi OS bude tedy relativně snazší monitorovat chování námi vydefinovaných politik v produkčním prostředí.

4 NÁVRH ŘEŠENÍ

Tato kapitola obsahuje návrh řešení zabezpečení systému Windows Server 2016.

Jelikož je požadavkem investora spolehlivé a prověřené řešení, které budeme moci nabízet klientům firmy, opřeme se při definování hodnot o bezpečnostní benchmarky vydávané organizací Center for Internet Security (CIS). Hodnoty z těchto materiálů poté aplikujeme do testovacího prostředí a budeme zjišťovat, které z bezpečnostních politik je třeba upravit podle specifikací zákaznických serverů.

Nejdříve je tedy nutné zajistit CIS benchmark pro Windows Server 2016. Dále zavést testovací prostředí. Jelikož pracujeme s doménovými politikami, budu nutná instalace minimálně jednoho řadiče domén a jednoho členského serveru. V této části práce také uvedu instalaci a základní konfiguraci OS Windows Server 2016.

Další fází bude postupné nastavování politik podle CIS benchmarku a sledování funkčnosti aplikací a služeb. V případě selhání některé pro nás kritické aplikace nebo služby, bude následovat identifikování zodpovědné politiky a upravení jejího nastavení, případně úplné vyřazení této politiky z bezpečnostního standardu XYZ, spol., s.r.o.

Po těchto úpravách nastavené politiky exportujeme, uvedeme testovací doménu do původního stavu po instalaci a základní konfiguraci a otestujeme import politik.

V případě úspěšného importu bude další fází zjištění konečného počtu bezpečnostních deviací, porovnání těchto deviací s hodnotami doporučenými CISem a zhodnocení výsledného skóre – tyto kroky provedeme s pomocí programu CIS-CAT.

Dále popíši modifikaci programu CIS-CAT, který jsem pro potřeby společnosti upravila tak, aby jej mohli zákazníci použít pro kontrolu, zda hodnoty na jejich serverech odpovídají standardům XYZ, spol. s.r.o.

Na závěr se zmíním o zpracování dokumentace a distribuci bezpečnostního standardu ve formě balíčku zákazníkům.

4.1 Předpoklady pro security hardening

4.1.1 CIS Windows Server 2016 benchmark

Pro získání CIS benchmarků, je potřeba být členem jejich online komunity. Členství je možné pro jednotlivce i firmy. Příspěvky, ať už finanční nebo jiné, jsou dobrovolné, jsou zde ovšem určitá omezení pro neplatící členy. Například program CIS-CAT, který budeme v rámci projektu používat, je omezen na 14denní zkušební verzi.

Společnost XYZ, spol. s.r.o. je dlouholetým členem CIS komunity a přispívá do ní jak peněžními dary, tak odborným poradenstvím a znalostmi. Není tedy problém se jednoduše přihlásit přes jejich stránky https://www.cisecurity.org/ a stáhnout potřebné materiály.

4.1.2 Testovací prostředí

Pro účely testování byla zavedena malá doména obsahující 2 řadiče domén (DC1 a DC2) a 2 členské servery (MS1 a MS2). Je důležité uvést, že tato doména je oddělena od produkčního prostředí nejen virtuálně, ale také fyzicky.

Pro virtualizaci prostředí byl použit program VM Ware ESXi 6.5.

4.2 Příprava testovacího prostředí

4.2.1 Instalace a základní konfigurace Windows Server 2016

Instalace Windows Server 2016 se nijak výrazně neliší od předchozích verzí. Celý proces instalace je možné najít v příloze 1 – popisuji zde instalaci OS s GUI (kvůli přehlednosti a s ohledem na skutečnost, že tato instalace je zákazníky společnosti nejčastěji požadovaná).

V rámci požadavku na novou instalaci se také řeší, zda bude server fyzický nebo virtuální, v případě virtuálního serveru je dále určeno, zda se pro jeho zavedení použije VM Ware

nebo Hyper-V. Vzhledem k zaměření této práce toto rozhodnutí pro nás není podstatné, nebudu se jím tedy zabývat.

Více se tedy budu věnovat konfiguraci typické pro většinu serverů společnosti XYZ spol. s.r.o.

V případě virtuálního serveru běžícího na VM Ware ESXi 6.5, s instalací WS 2016 s grafickým rozhraním bude konfigurace následující.

Naším prvním krokem bude konfigurace sítě – zakázání IPv6 a všech tunelovacích protokolů (teredo, isatap a 6TO4), nastavení vhodné IPv4, preferovaných DNS serverů (jak hlavního, tak alternativního). Dále nás také čeká výběr jména domény a hesla, ideálně přejmenování serveru, abychom jej mohli v doméně snadno identifikovat.

Druhým krokem je samotná instalace Active Directory Domain Services. Ta je podrobně popsaná v příloze 2.

Jakmile máme nainstalované AD DS, čeká nás instalace aplikací a softwaru třetích stran potřebných pro monitoring, správu, sdílení souborů nebo například tisk. Musíme také vytvořit doménové uživatele a vydefinovat jim oprávnění.

Při vytváření uživatelů v testovací doméně zohledníme uživatele, skupiny a oprávnění aplikované v produkčním prostředí. V našem případě jsou v produkci standardně zavedeny 2 skupiny pro správu domény s odlišnými oprávněními. Zavedeme tyto skupiny tedy i do testovacího prostředí a do každé umístíme alespoň 2 uživatele. Pro naše testovací účely bude takto předpřipravený řadič domén dostačující. Jak budu dále zmiňovat, potřebujeme do testovacího prostředí i členské servery. Jejich konfigurace bude podobná, až na instalaci AD DS – tu nahradíme prostým připojením počítače do domény.

4.2.2 Instalace Group Policy Management konzole

Součástí každé instalace OS Windows je Local Group Policy Editor (Editor místních zásad skupiny, dále jen LGPE), v němž se dají vydefinovat politiky pro tento jeden

server/klient. V případě stand-alone serverů je tento editor naprosto dostačují, avšak pro správu politik v rámci domény bude nezbytný nástroj, který nám umožní spravovat politiky všech členských serverů z řadiče domén najednou.

Pro nastavení a správu námi vydefinovaných doménových politik je naprosto nezbytná Group Policy Management Console (dále jen GPMC).

V případě novějších verzí Windows Server je doplněk GPMC automaticky zahrnutý při instalaci AD DS, není tedy třeba ji tu rozebírat.

Ve starších verzích konzoli můžeme naistalovat buď pomocí grafického rozhraní nebo pomocí následujícího příkazu: **ServerManagerCmd -install gpmc**.

4.2.3 Předpoklady pro úpravu politik v GPMC

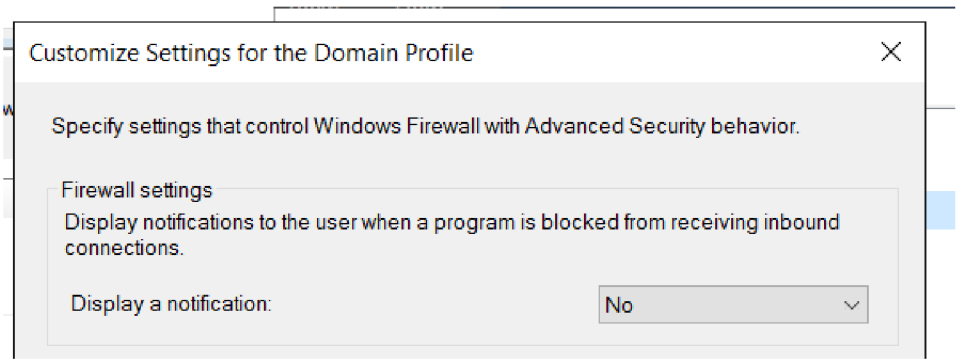
Jelikož je cílem jednotná sada politik pro serverové prostředí, vytvoříme jeden Group Policy Object (GPO) v organizační jednotce dle našeho uvážení, a s ohledem na strukturu spravované domény.

V průběhu nastavování námi požadovaných hodnot jsme také narazili na několik problémů se zobrazením či neexistencí některých politik. Řešením těchto problémů se zabývají následující 2 kapitoly.

Šablony ADMX

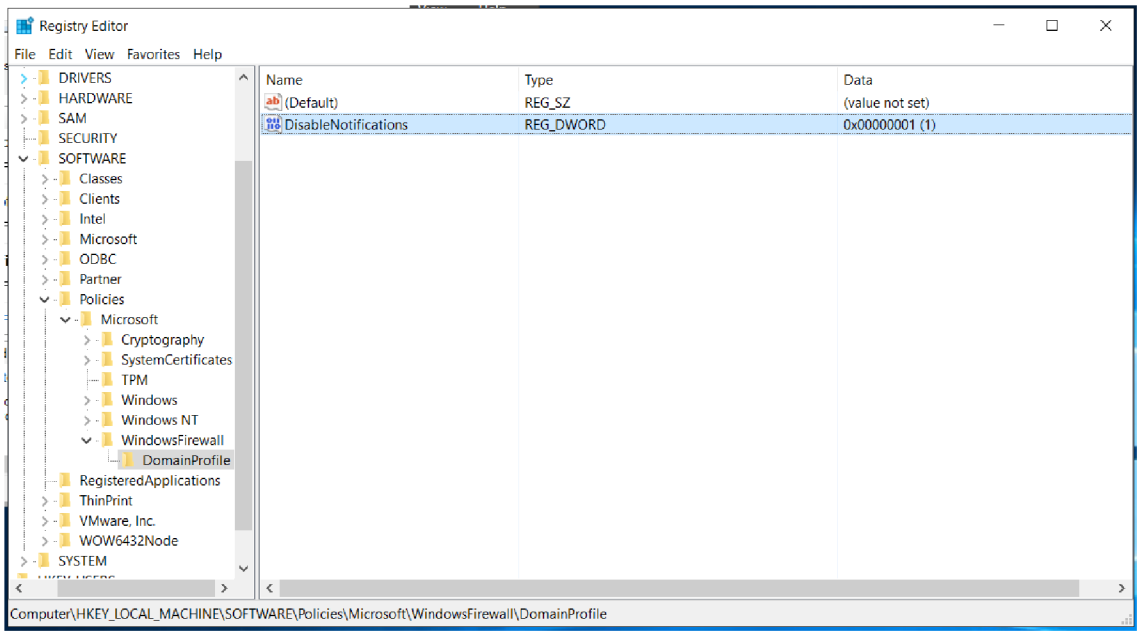
Šablony ADMX jsou soubory, pomocí nichž můžeme konfigurovat jednotlivé politiky v registrech. Součástí instalace OS Windows je balíček, který obsahuje převážnou většinu těchto souborů. Pokud ovšem některá z šablon chybí, nebudeme schopní korespondující politiku nakonfigurovat pomocí GPMC. Museli bychom jít přes registry, což by nebyl problém, pokud by nám chyběla jedna nebo dvě politiky. V našem případě jich ovšem chybělo deset. Nastavovat větší množství politik přímo přes registry je časově náročné, nepřehledné a náchylnější k chybám, jelikož názvy politik v registrech jsou zkrácené a neodpovídají názvům (a někdy ani logice) v GPMC nebo Local Group Policy Editoru.

Například CIS politika *„9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Scored)“* vypadá v GPMC takto:



Obr. 3: Politika Windows Firewall: Domain Settings: Display a notification v GPMC (Zdroj: vlastní zpracování)

A v registrech takto:



Obr. 4: Politika Windows Firewall: Domain Settings: Display a notification v registrech (Zdroj: vlastní zpracování)

No/Yes u převážné většiny pravidel odpovídají hodnotám 0/1. Pokud je ovšem název politiky v registrech obrácen způsobem uvedeným na Obr. 4, pak v GPMC ve vztahu k registrům No=1 a Yes=0, čehož bychom si nemuseli všimnout.

Je tedy bezpečnější chybějící šablony ADMX doinstalovat.

Prvním krokem bude nalezení a stažení šablon z webových stránek společnosti Microsoft. Lze zde najít balíčky veškerých politik dostupných pro konkrétní OS.

Jakmile máme stažené odpovídající šablony jsou 2 způsoby, jak je nainstalovat.

1. Můžeme šablony jednoduše umístit do složky, čímž dosáhneme toho, že budou viditelné na řadiči domén, na němž pracujeme, ale nebudeme schopní tyto politiky vidět v Local Group Policy Editorech ostatních serverů v doméně, což platí jak pro členské servery, tak pro záložní řadiče domén.
2. Druhým způsobem je vytvořit Central Store – složku zajišťující replikaci .admx a .adml souborů na ostatní členy domény.

   S ohledem na požadavky a preference zákazníků firmy jsem v rámci tohoto projektu zahrnula do dokumentace i návod na vytvoření Central Storu, který jsem ve fázi testování i vytvořila a vyzkoušela.

   Návod na vytvoření a zprovoznění Central Storu se nachází v příloze 3.

Zobrazení MSS: Microsoft Security Standard v GPMC

Microsoft Security Standard je skupina asi 20 hodnot z registrů, které historicky předcházejí skupinové politiky a nejsou automaticky zařazeny do editorů na správu politik. Jelikož jsou tato nastavení z hlediska bezpečnosti kritická a budeme je chtít modifikovat, je nutné je do těchto editorů přidat (ať už pracujeme s GPMC nebo LGPE).

Návod na zobrazení těchto nastavení je k nalezení v příloze 4.

4.2.4 Vytvoření Snapshotů

Vzhledem k tomu, že po exportu politik budeme potřebovat otestovat import našeho nastavení do neupravené instalace WS 2016, musíme se rozhodnout, zda projít procesem

instalace a konfigurace znovu, nebo vytvořit snapshot, pomocí něhož se pak vrátíme do základního stavu.

Jelikož je toto pouze testovací prostředí, můžeme si dovolit využít funkce vytvoření snapshotu programu VM Ware. Snapshot je forma zálohování virtuálního systému, která je ovšem závislá na existenci této virtuální jednotky. Nelze jej tedy zaměňovat s klasickou zálohou. V případě, že virtuální stroj vymažeme, zničí se spolu s ní i snapshot, což pro klasické zálohování neplatí.

V produkčním prostředí by využití snapshotů bylo zvláště pro řadiče domén nepřijatelné. Mohou nastat problémy s replikacemi z důvodu narůstajících USN identifikátorů, pak by nemuselo být možné doménu znovu zprovoznit. Toto riziko je pro nás ovšem přijatelné. Pokud se obnovení ze snapshotů v pozdější fázi nepodaří, neztratíme tím žádná důležitá data.

4.3 Testování

Vzhledem k citlivosti jakýchkoliv informací z oblasti bezpečnosti sítí, požadavku společnosti XYZ spol. s.r.o. zůstat v anonymitě a chránit interní informace a s ohledem na licenční dohody vztahující se k materiálům třetích stran, které v této práci používám, budu uvádět pouze příklady vybraných nastavení. Některá z těchto nastavení také mohou být pozměněna.

4.3.1 Nastavení hodnot podle CIS benchmarku

Při práci s politikami v GPMC budeme pracovat s následujícími podkategoriemi ve větvi Computer configuration (konfigurace počítače):

- Account Policies (zásady účtů),
- Advanced Audit Policy Configuration (zásady auditování systému),
- Security Options (možnosti zabezpečení),
- User Rights Assignments (přiřazení uživatelských práv),
- Administrative templates (šablony pro správu),

- MSS settings (nastavení MSS),
- Windows Firewall with Advanced Security (brána Windows Firewall s pokročilým zabezpečením).

Těmto skupinám budou přiřazeny troj číselné identifikátory, podle nichž bude každé nastavované politice přiděleno unikátní ID pro větší přehlednost mimo jiné i při zpracovávání dokumentace.

Account policies – nastavení týkající se účtů (délka a komplexnost hesla, jak často heslo měnit, po kolika pokusech se uzamkne účet a na jak dlouho, …).

Advanced audit policy configuration – veškeré politiky týkající se auditování a zápisů v rámci domény (jaké informace se mají ukládat, kam a jak často, včetně podmínek spuštění těchto zápisů).

Security Options – nejobsáhlejší větev politik, nastavení jako je například přejmenování Administrator a Guest účtu, omezení NTLM protokolu, pravidla pro UAC (kontrola uživatelských účtů) nebo konfigurace síťového přístupu.

User Rights Assignments – způsoby jakými se může uživatel přihlásit do systému, přiřazení určitých činností pouze některým skupinám, vlastnictví souborů a složek.

Administrative templates – politiky využívající .admx a .adml šablony.

MSS settings – původní bezpečnostní nastavení společnosti Microsoft, zařadit je lze do kategorie Security Options, odděleně jsou hlavně kvůli přehlednosti.

Windows Firewall with Advanced Security – nastavení služby Windows Firewall s pokročilým zabezpečením (zda je služba zapnutá, definování úložiště a velikosti záznamů, nastavení výjimek). Nastavíme tedy na náš řadič domén hodnoty politik v těchto kategoriích podle hodnot vydefinovaných CISem v benchmarku pro Windows Server 2016 a budeme sledovat reakci našeho testovacího prostředí na tyto politiky.

4.3.2 Sledované charakteristiky

V rámci testování budeme postupně ověřovat a kontrolovat funkčnost následujících aplikací, služeb a programů:

- Program pro monitoring,
- Program pro správu serverů,
- PS remoting,
- Remote Desktop Control,
- RSAT (Remote Server Administration tool) – program na vzdálenou správu serverů, testování funkčnosti mezi 2 členskými servery a mezi členským serverem a řadičem domén,
- Server manager – kontrola služeb a událostí,
- AD uživatelé a počítače,
- Sdílení souborů, DFS replikace,
- Tiskový server (sdílená tiskárna, tisk přes síť),
- IIS.

Dále je také nutné kontrolovat replikaci doménových politik na záložní řadič domén a také na naše dva členské servery.

4.3.3 Bezpečnostní odchylky

V závěru testování bychom měli mít seznam politik, které jsme upravili společně s důvodem pro jejich modifikaci.

Z každé skupiny námi definovaných politik jsem náhodně vybrala jednu nebo dvě takové politiky, aby se jejich hodnoty lišily od hodnot doporučených CIS. Pokusím se dále vysvětlit důvody těchto bezpečnostních odchylek a jejich potenciální dopad.

Tab. 2: Bezpečnostní odchylky (Zdroj: Vlastní zpracování)

Politika	**CIS**	**XYZ, spol. s.r.o.**	**Důvod odchylky**
Account lockout duration	15	30	Bylo usouzeno, že hodnota 15 je příliš nízká.
Audit Policy: Logon-Logoff: Account Lockout	Success	Success and Failure	Požadavek na auditování i neúspěšných událostí.
Audit Policy: Logon-Logoff: Other Logon/Logoff Events	Success and Failure	No Auditing	Nastavení generuje zbytečně velké množství záznamů, které jsou převážně nepotřebné.
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled	Disabled	Riziko negativního dopadu na uživatele v případě nedostupnosti řadiče domén.
Microsoft network server: Digitally sign communications (always)	Enabled	Disabled	Nastavení je nekompatibilní se staršími OS, které jsou zákazníky

			ještě hodně používány.
Act as part of the operating system	No One	Administrators	Potřebné pro funkčnost některých interních nástrojů.
Include command line in process creation events	Disabled	Enabled	Záznam z této politiky může být kritický pro vyšetřování bezpečnostních událostí. Tento záznam je přístupný pouze administrátorům.
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	5	0	Bylo usouzeno, že hodnota 5 je příliš vysoká.
Windows Firewall: Domain: Firewall state	On	Off	Využití HW firewallů 3. stran.

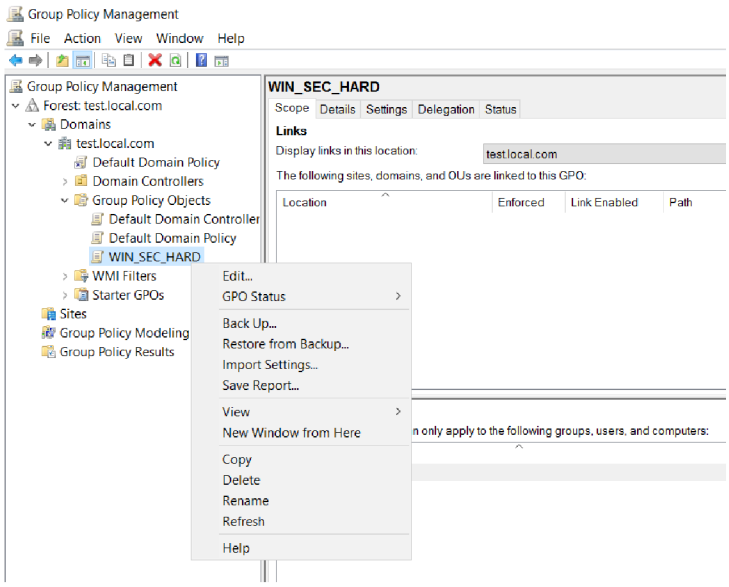
4.4 Export a import

Export a import politik zajistíme přes GPMC konzoli, kterou jsme nainstalovali v rámci instalace AD DS.

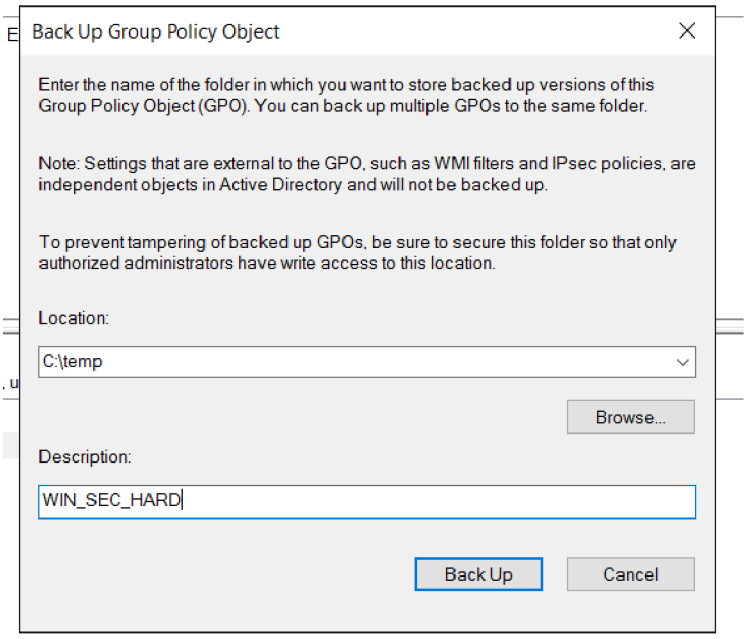
4.4.1 Export politik

Jakmile máme všechny nastavené hodnoty otestovány a překontrolovány, je potřeba je vyexportovat, abychom je mohli využívat v interním prostředí a také nabízet jako balíček zákazníkům.

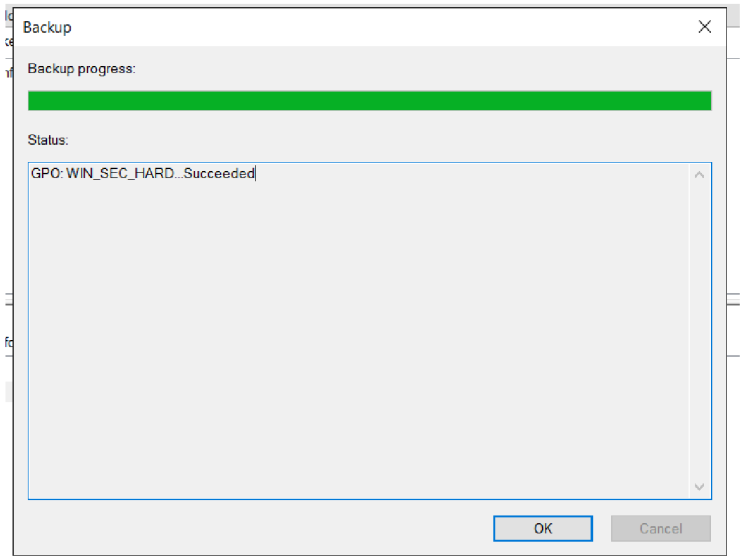
Export politik provedeme pomocí funkce Back up… jak je zobrazeno na následujících obrázcích.



Obr. 5: Export nastavení 1 (Zdroj: Vlastní zpracování)



Obr. 6: Export nastavení 2 (Zdroj: Vlastní zpracování)



Obr. 7: Export nastavení 3 (Zdroj: Vlastní zpracování)

Výsledkem je složka, která obsahuje veškerá nastavení politik a lze ji jednoduše zabalit do archivu a distribuovat mezi servery.

4.4.2 Obnovení ze snapshotu

Jakmile máme vyexportované politiky úspěšně stažené z našich testovacích serverů, můžeme všechny 4 virtuální systémy obnovit ze snapshotů

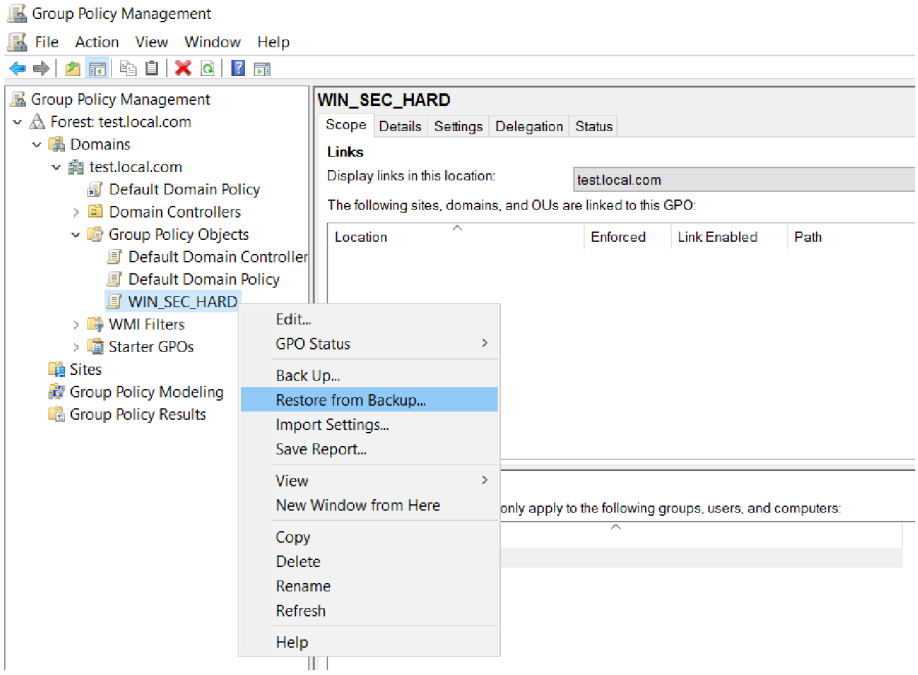
Jak jsem již uvedla výše, je zde pro řadiče domén riziko, že se nám doménu nepodaří uvést do původního stavu a budeme muset instalovat a konfigurovat testovací prostředí znovu.

Toto se v našem případě ovšem nepotvrdilo, jelikož se obnova bez problémů podařila a doména v pořádku funguje. Můžeme tedy přejít k importu našich nastavení.

4.4.3 Import politik

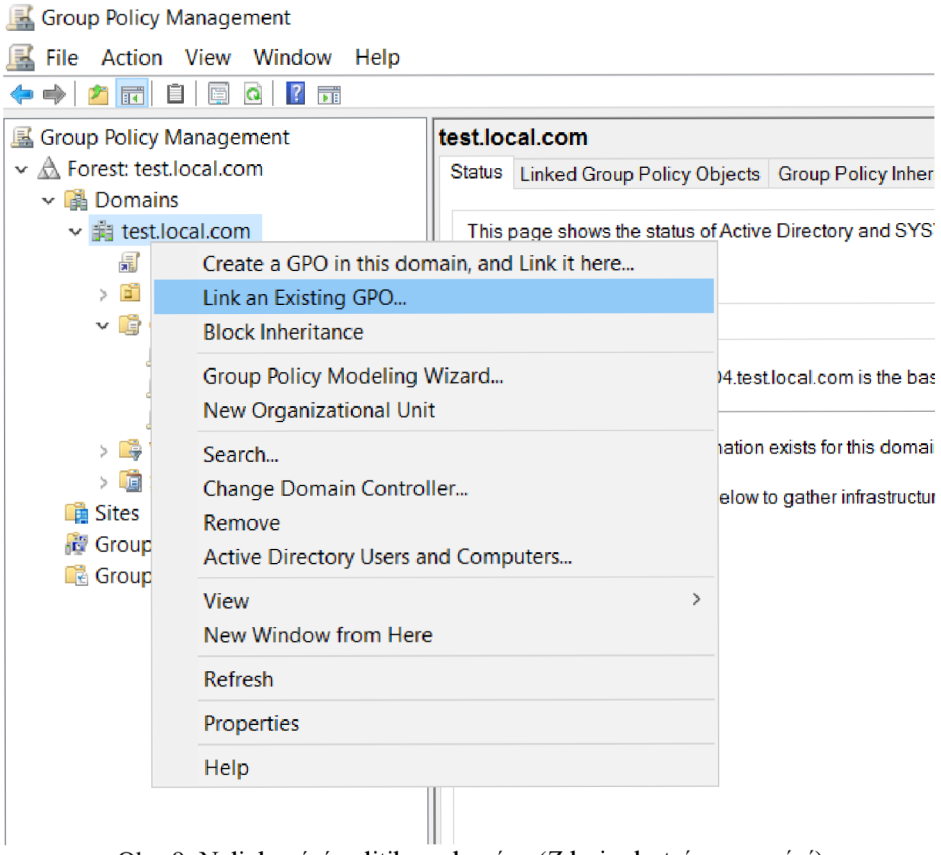
Import politik zajistíme velice podobně jako export. V GPMC konzoli vytvoříme nový Group Policy Object a pojmenujeme ho.

Klikneme na pravým a pomocí funkce Restore from Backup… vyhledáme v systému, kam jsme vyexportovanou politiku uložili a tímto ji naimportujeme.



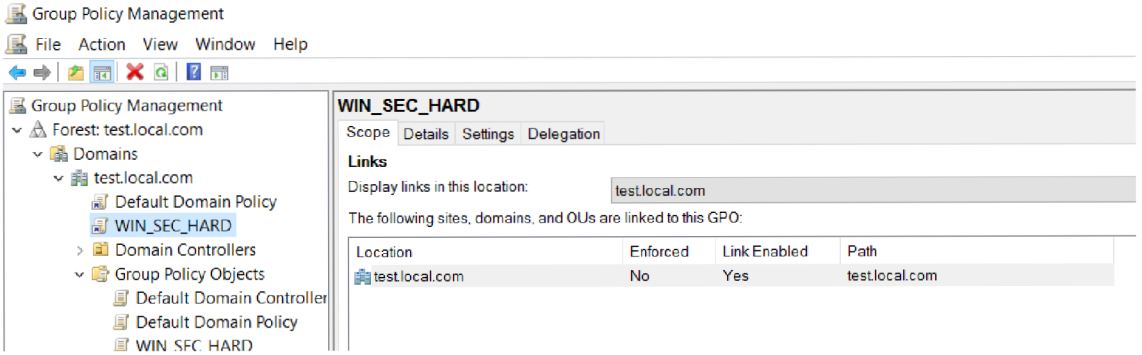
Obr. 8: Import nastavení (Zdroj: vlastní zpracování)

Pro aplikaci politik je nutné je na naši doménu nalinkovat.

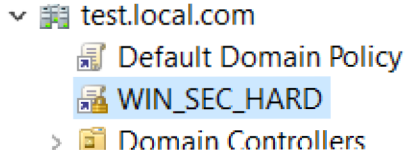


Obr. 9: Nalinkování politik na doménu (Zdroj: vlastní zpracování)

A jelikož chceme, aby byla použita všechna nastavení v ní obsažena, využijeme ještě možnosti Enforced. Tím zajistíme, že se budou upřednostňovat naše hodnoty před nastaveními obsaženými například v Default Domain Policy.



Obr. 10: Politiky aplikované na doménu test.local.com (Zdroj: vlastní zpracování)



Obr. 11: Zlatý zámek označuje politiku jako Enforced (Zdroj: vlastní zpracování)

Závěrem zkontrolujeme přímo na členských serverech a záložním řadiči domén, zda se nastavení zdědila v rámci celé domény.

4.5 Kontrola a práce s programem CIS-CAT

Jako kontrolní nástroj jsme zvolili program CIS-CAT vytvořený CISem za účelem analýzy nastavení bezpečnostních politik systémů. Pro jeho použití je třeba pouze doinstalovat Javu, která je zdarma dostupná na adrese https://www.java.com/en/.

4.5.1 Bezpečnostní deviace

Pro zjištění veškerých bezpečnostních deviací využijeme zprávu vygenerovanou programem CIS-CAT. Celý postup práce s CIS-CATem je uveden v příloze 5. Zde se zaměřím pouze na výslednou zprávu.

CIS-CAT dává možnost vygenerování zprávy ve formátu .html, .csv a .xml. Pro práci a univerzálnost dat je nejlepší formát .csv, ovšem my se zaměříme na přehlednost a využijeme tedy .html formát.

Na následujícím obrázku je příklad výsledku kontroly systému.

Summary

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Account Policies	[redacted]						**78%**
1.1 [redacted]	5	1	0	0	5.0	6.0	83%
1.2	2	1	0	0	2.0	3.0	67%
2 Local Policies	[redacted]						**59%**
2.1 [redacted]	0	0	0	0	0.0	0.0	0%
2.2	22	15	0	0	22.0	37.0	59%
2.3	38	27	0	0	38.0	65.0	58%
19.7.42 [redacted]	0	0	0	0	0.0	0.0	0%
19.7.43	0	0	0	0	0.0	0.0	0%
19.7.43.1	0	0	0	0	0.0	0.0	0%
19.7.43.2	0	0	0	0	0.0	0.0	0%
Total	[redacted]						**28%**

Obr. 12: Příklad kontroly systému pomocí programu CIS-CAT (Zdroj: vlastní zpracování)

Z podobného přehledu získáme data k sestavení přehledu všech deviací, čímž získáme i jejich počet a váhu ve výsledném skóre.

4.5.2 Výsledné skóre

Výsledné skóre lze zjistit z .html reportu, který jsme vygenerovali v předchozím kroku.

CIS rozděluje politiky na scored a unscored. Kritická jsou scored zabezpečení, která se započítávají do výsledného skóre. Unscored politiky je třeba chápat spíše jako doporučení, do výsledného skóre se nezapočítávají.

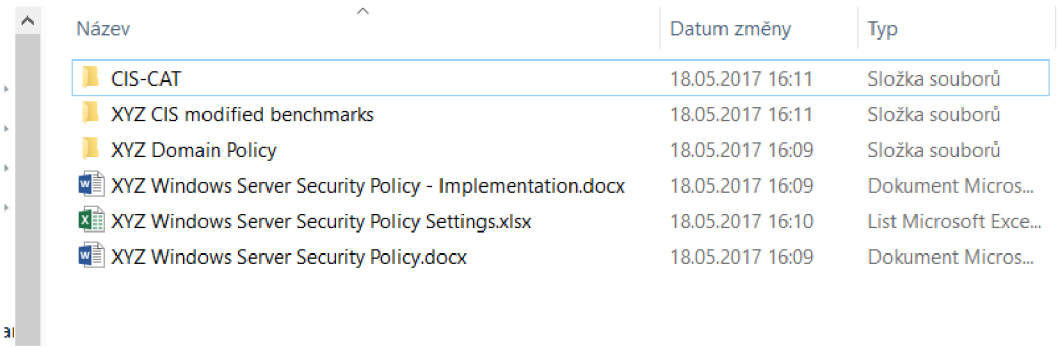
Po všech úpravách nezbytných pro specifikace našeho zákaznického prostředí jsme dosáhli skóre 76,3 %.

4.6 Modifikace CIS benchmarků

Další fází projektu bude úprava benchmarků poskytnutých CISem na hodnoty bezpečnostního standardu společnosti XYZ, spol. s.r.o. tak, abychom mohli takto upravené soubory společně s programem CIS-CAT distribuovat dále naším zákazníkům jako formu kontroly a analýzy systému.

4.7 Dokumentace a distribuce zákazníkům

Zákazníkům budeme politiky distribuovat jako součást balíčku, který obsahuje také veškerou dokumentaci, a také program CIS-CAT společně s benchmarkem, který byl modifikován na hodnoty bezpečnostního standardu XYZ, spol. s.r.o.



Obr. 13: Obsah balíčku XYZ Security Standard (Zdroj: vlastní zpracování)

4.8 Přínosy řešení

Jelikož naše řešení není komerční produkt a nebude nabízen za úplatu, přímé přínosy nelze kvantifikovat, bezpochyby se ale zvýší kvalita služeb poskytovaných klientům. V následujících kapitolách se tedy zaměřuji na kvalitativní přínosy řešení.

4.8.1 Zvýšení informační bezpečnosti a důvěry klientů

Distribucí našich politik mezi co nejvyšší počet zákazníků se zajistí zvýšení zabezpečení nejen klientských serverů, ale i firemního prostředí. Zvýší se tedy celková informační bezpečnost i bezpečnost zákaznických dat, což by mělo mít pozitivní vliv na důvěru zákazníků ve společnost.

4.8.2 Snížení nákladů na servisní zásahy u klientů

Předpokládaný je také snížený počet bezpečnostních incidentů a událostí, a tím také menší zatížení pro tým zajišťující zákaznickou podporu a bezpečnostní tým a výsledné snížení nákladů na servisní zásahy u klientů.

4.8.3 Vytvoření konkurenční výhody

Dalším očekávaným přínosem je výhoda oproti konkurenci. Z průzkumu trhu bylo zjištěno, že v oboru je takovéto řešení bezpečnosti spíše výjimkou. Pokud je zákazníkům nabízen nějaký podobný produkt, tak je většinou zdlouhavě implementován, pro zákazníka je drahý a vzhledem k absenci podrobné dokumentace složitý na správu.

4.8.4 Metodika pro budoucí hardeningy

Přínosem je také fakt, že při implementaci bezpečnostních pravidel individuálních zákaznických řešení, již není třeba začínat od nuly, pouze importovat a otestovat námi navržený bezpečnostní standard, případně modifikovat politiky, které negativně ovlivňují funkčnost zákaznického prostředí. Jde tedy o nezanedbatelnou úsporu času, díky které se firmě sníží náklady na zákazníka.

Samotná bakalářská práce bude sloužit jako určitý zdroj interní dokumentace a současně jako obecný návod pro budoucí bezpečnostní hardeningy.

ZÁVĚR

Cílem mé práce bylo navrhnout funkční a efektivní řešení security hardeningu operačního systému Windows Server 2016 v prostředí společnosti XYZ, spol. s.r.o. Hlavním problémem bylo adekvátní vyvážení otázky bezpečnosti a dostupnosti dat.

Jako hlavní podklad sloužily security benchmarky neziskové organizace CIS, stejně jako program CIS-CAT využitý pro analýzu systému.

K dispozici bylo testovací prostředí, kde bylo možné provedené změny průběžně zkoušet a v případě potřeby rušit a navrátit se k původnímu stavu.

Navrhované řešení je momentálně využíváno pro interní potřeby společnosti a začíná se postupně i nabízet zákazníkům. Jako ověřený postup jej bude možné v budoucnu používat jako vzor pro hardeningy dalších operačních systémů.

SEZNAM POUŽITÝCH ZDROJŮ

(1) BRAGG, Roberta. *Hardening Windows systems.* New York, N.Y.: McGraw-Hill/Osborne, c2004. ISBN 0072253541.

(2) HASSELL, Jonathan. *Hardening Windows.* New York: Distributed to the Book trade in US by Springer-Verlag, c2004. ISBN 1590592662.

(3) CIS Security. *Cisecurity.org* [online]. [cit. 2016-04-22]. Dostupné z: https://www.cisecurity.org/

(4) VeritLabs. 20 Years of Windows Server Product History. *Veritlabs.com.* [online]. [cit. 2016-04-22]. Dostupné z: http://www.veritlabs.com/20-years-of-windows-server-product-history/

(5) Microsoft Corporation. Data Security and Data Availability in the Administrative Authority. *Msdn.microsoft.com* [online]. [cit. 2016-04-22]. Dostupné z: https://msdn.microsoft.com/en-us/library/cc722918.aspx

(6) Microsoft Corporation. A history of Windows. *Windows.microsoft.com* [online]. [cit. 2016-04-22]. Dostupné z: http://windows.microsoft.com/en-us/windows/history

(7) CIS Security. Security Benchmarks. *community.cisecurity.org* [online]. [cit. 2016-04-22]. Dostupné z: https://community.cisecurity.org/

(8) DESMOND, Brian, Joe RICBARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. Active Directory. 5th edition. Sebastopol: O'Reilly Media, 2013. ISBN 978-1-449-32002-7.

(9) MOSKOWITZ, Jeremy. Group policy: fundamentals, security, and the managed desktop. 2nd ed. Indianapolis, Ind.: John Wiley and Sons, 2013.

(10) ROUNTREE, Derrick. Security for Microsoft Windows system administrators: introduction to key information security concepts. Boston: Syngress, c2011. ISBN 1597495948.

(11) ROUNTREE, Derrick. a Richard. HICKS. Windows 2012 server network security: securing your windows network systems and infrastructure. Amsterdam: Elsevier, 2013. ISBN 9781597499583.

(12) STANEK, William R. Active Directory: kapesní rádce administrátora. Vyd. 1. Brno: Computer Press, 2009. Microsoft (Computer Press). ISBN 978-80-251-2555-7.

(13) O doménách a DNS. *NIC.cz* [online]. [cit. 2016-12-15]. Dostupné z: https://www.nic.cz/page/312/o-domenach-a-dns/

(14) Group Policy. *TechNet* [online]. [cit. 2016-12-15]. Dostupné z: https://technet.microsoft.com/cs-cz/windowsserver/bb310732.aspx

(15) GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 978-80-247-5457-4.

(16) Bezpečnost. Základní pojmy. *KYBEZ.cz* [online]. [cit. 2016-12-17]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

(17) POŽÁR, J. Základy teorie informační bezpečnosti. 1. vyd. Praha: Vydavatelství PA ČR, 2007, 219 s. ISBN 978-80-7251-250-8.

(18) Výpis s obchodního rejstříku. *JUSTICE.cz* [online]. [cit. 2016-12-17]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

CIS – Center for Internet Security

OS – Operační systém, Operating System

IS – Informační Systém

CIS-CAT – Center for Internet Security Configuration Assessment Tool

AD – Active Directory

LDAP – Lightweight Directory Access Protocol

DNS – Domain Name System

IP – Internet Protocol

FQDN – Fully Qualified Domain Name

TLD – Top-Level Domain

ADDS – Active Directory Domain Services

DC – Domain Controller

RODC – Read-Only Domain Controller

GPO – Group Policy Object

GPMC – Group Policy Management Console

IT – Information Technology

OR – Obchodní rejstřík

CEO – Chief Executive Officer

VM – Virtual Machine

CPU – Central processing unit

RAM – Random access memory

PDC – Primary Domain Controller

DHCP – Dynamic Host Configuration Protocol

RHEL – Red Hat Enterprise Linux

SLES – SUSE Linux Enterprise Server

WS – Windows Server

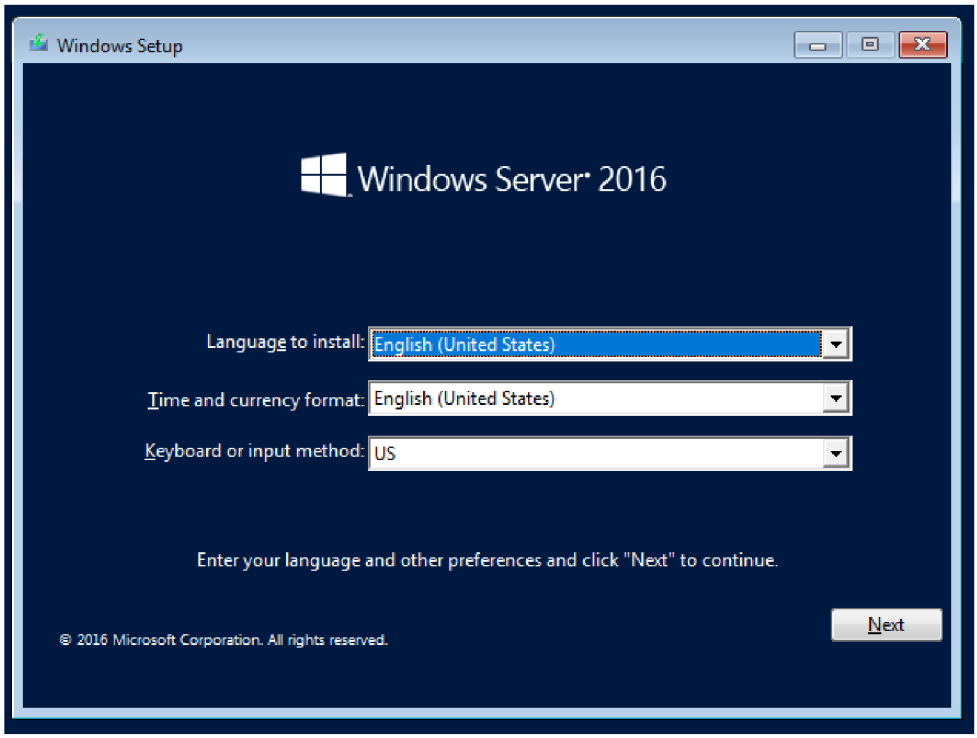
SEZNAM OBRÁZKŮ

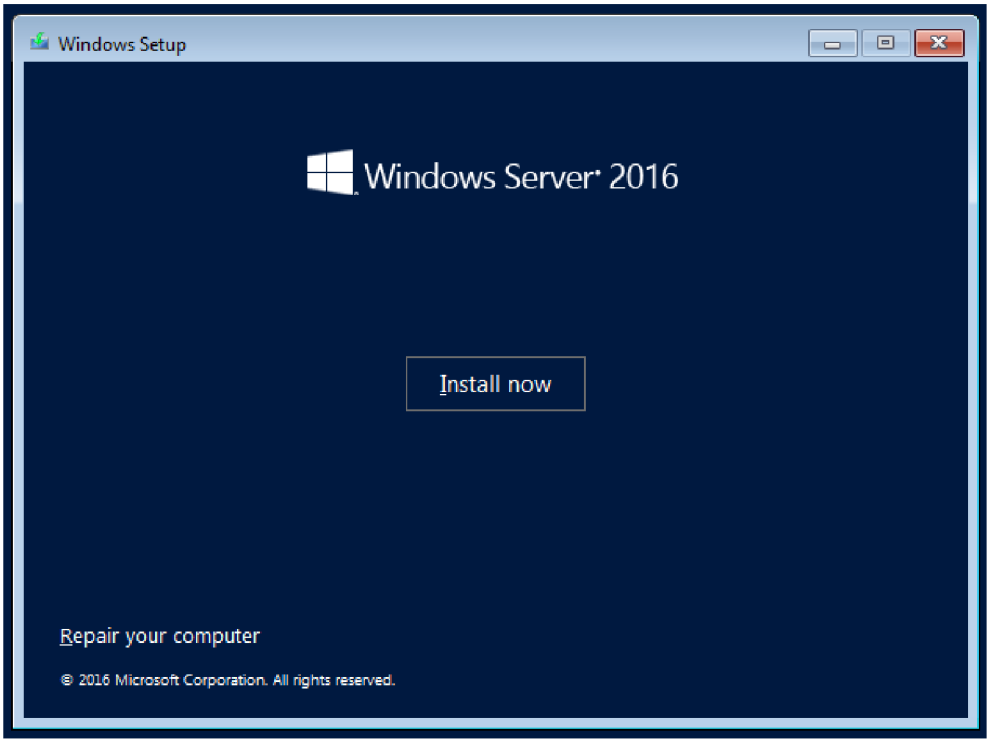
SEZNAM TABULEK

SEZNAM PŘÍLOH

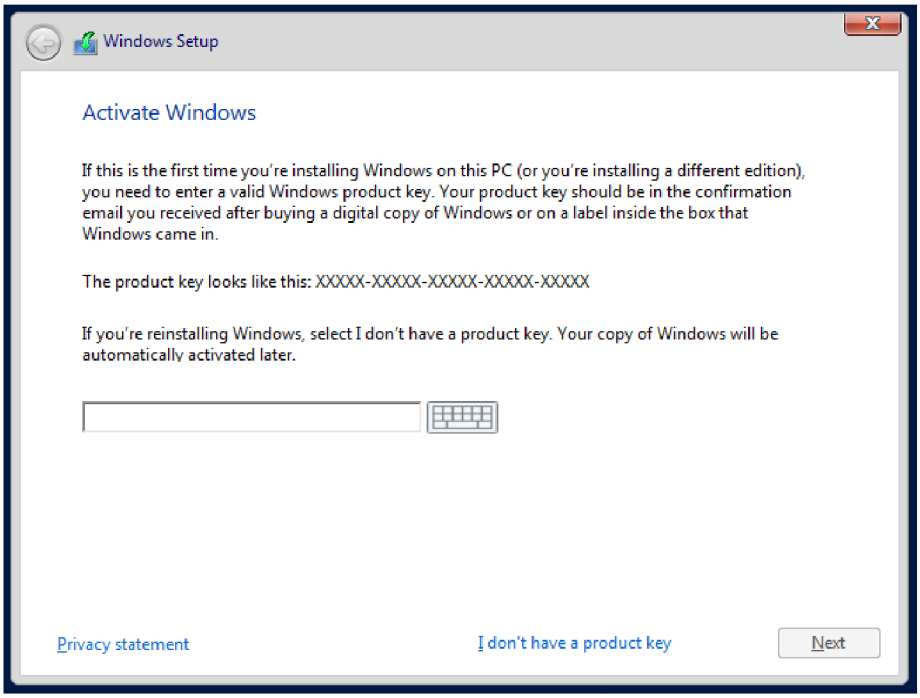
Příloha 1 - Instalace Windows Server 2016 s GUI

Instalace Windows Server 2016 je velice intuitivní, budu tedy uvádět poměrně málo poznámek k jednotlivým krokům.

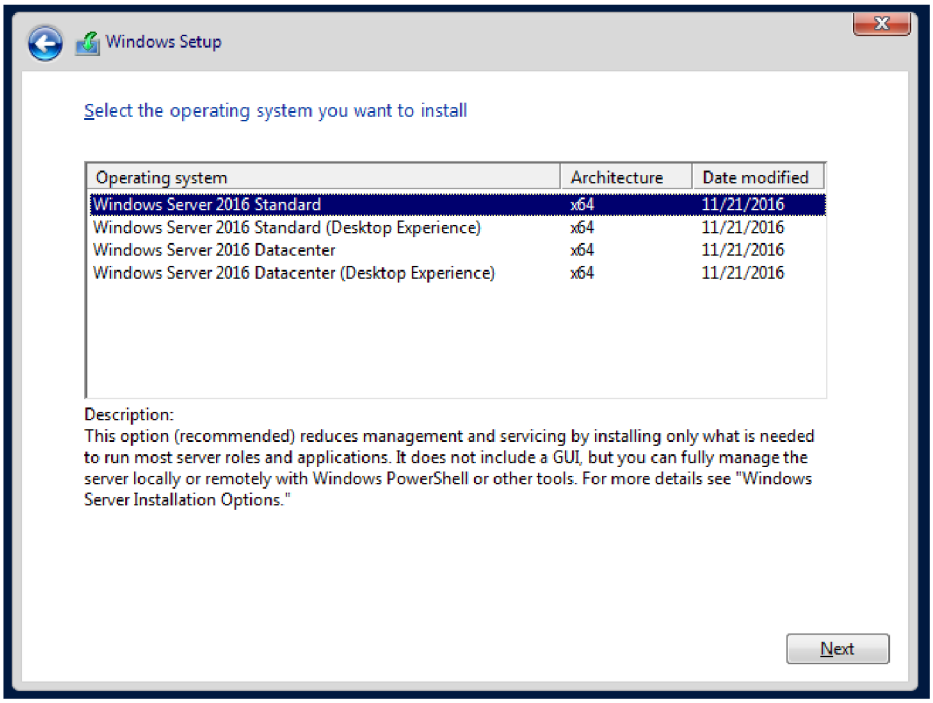




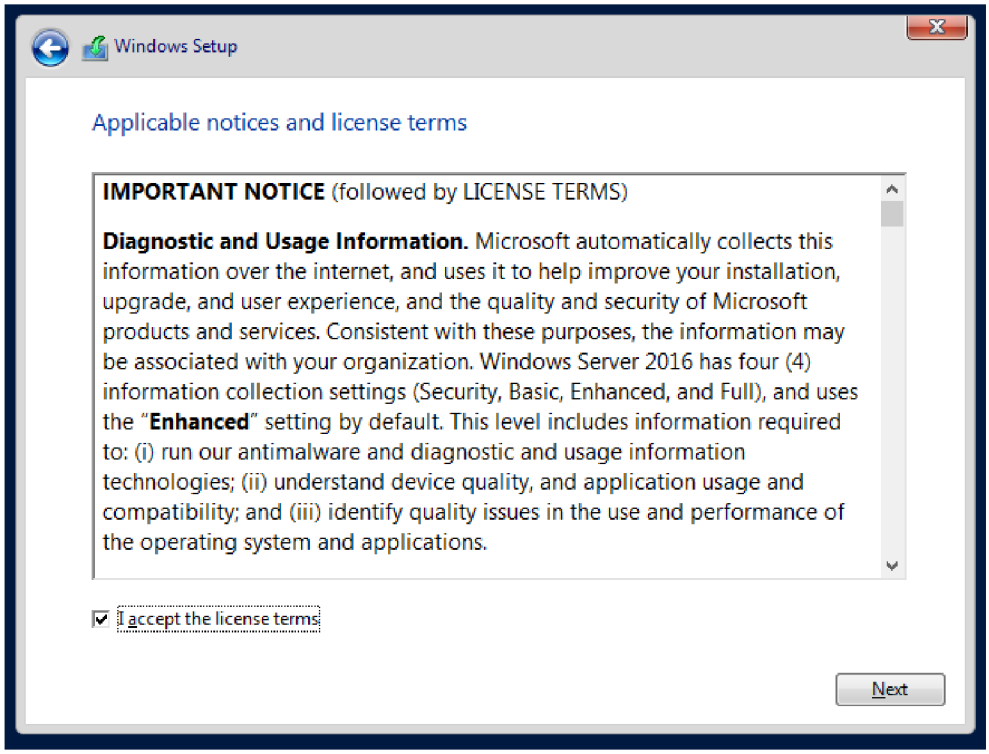
Pokud nemáme aktivační klíč, lze následující krok přeskočit a aktivovat Windows později.

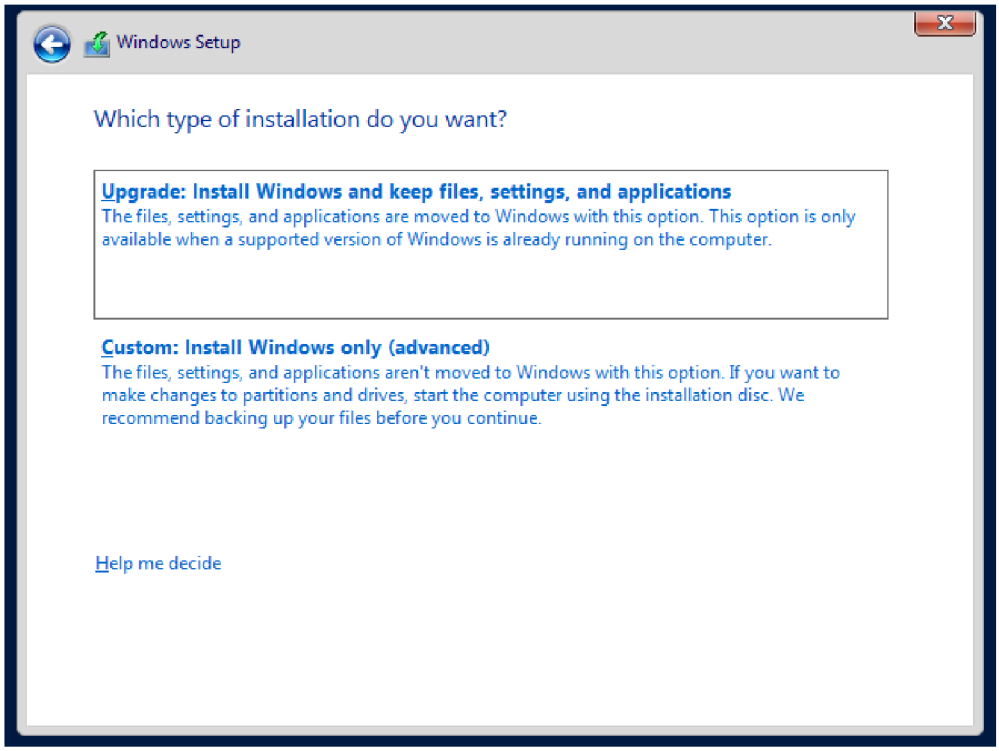


V téhle části vybereme, jakou verzi OS chceme. Poznámka v závorce „Desktop Experience“ nám říká, že toto je verze s GUI. Vybereme tedy 2. možnost.

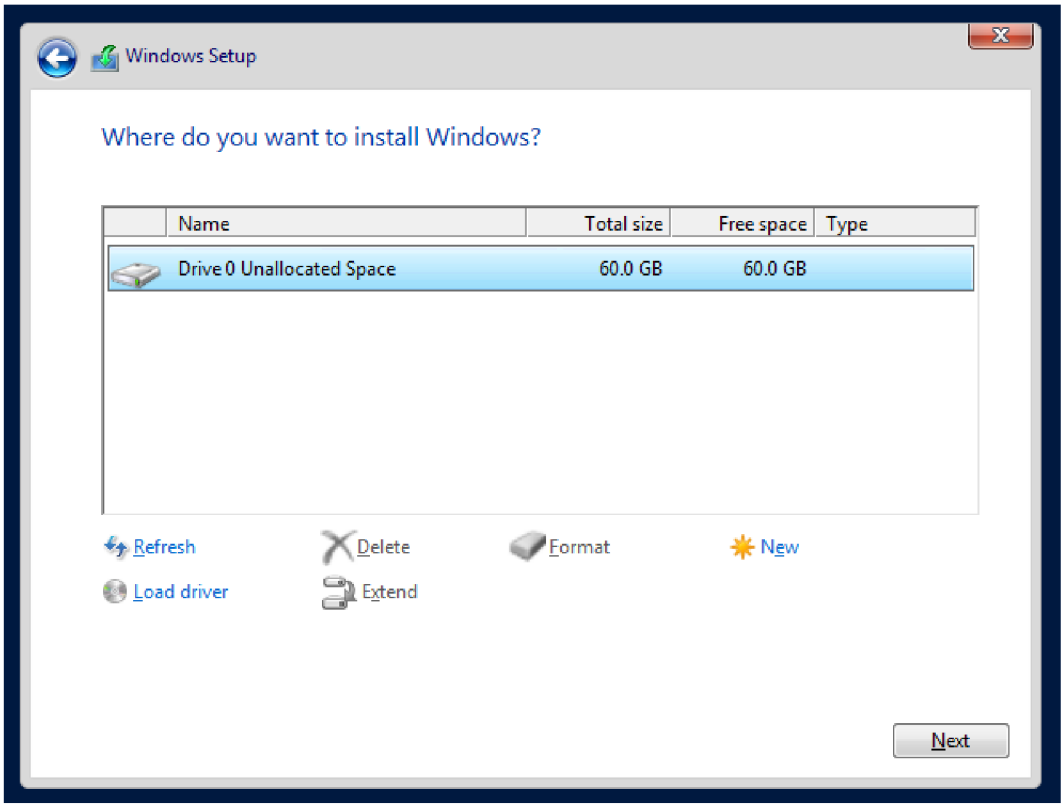


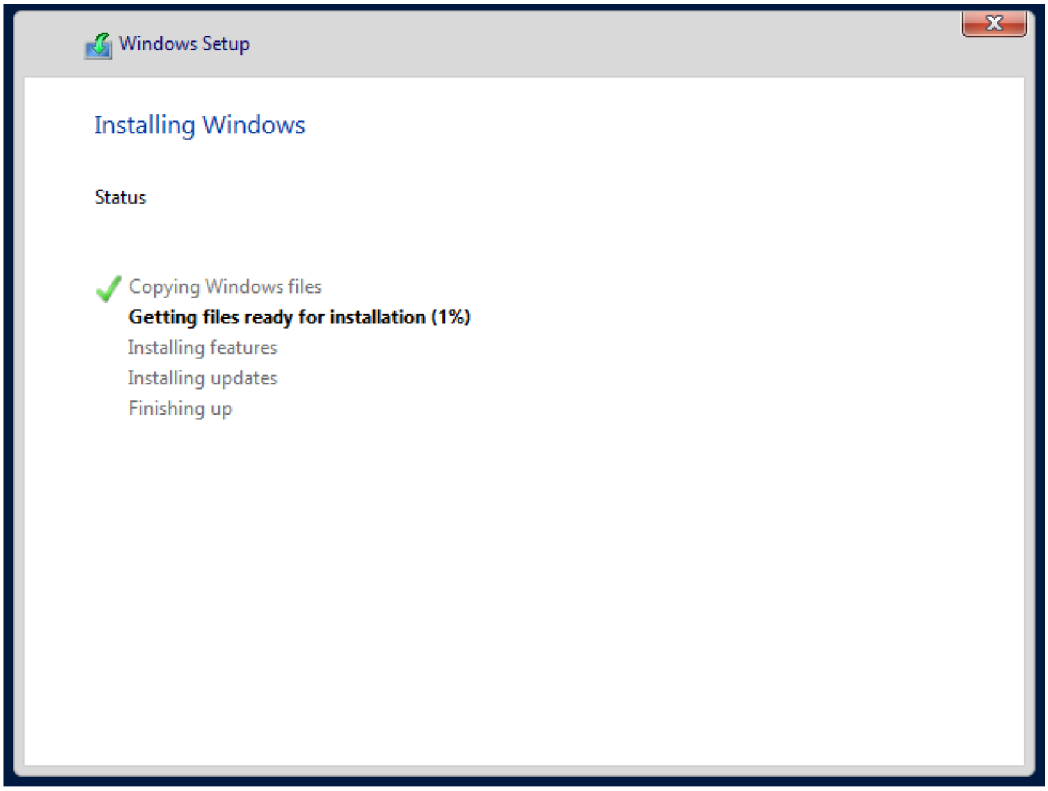
Zatrhneme položku „I accept the license terms“ čímž přijmeme licenční podmínky a v další kroku vybereme možnost „Custom: Install Windows only (advanced)“, jelikož chceme novou instalaci OS.



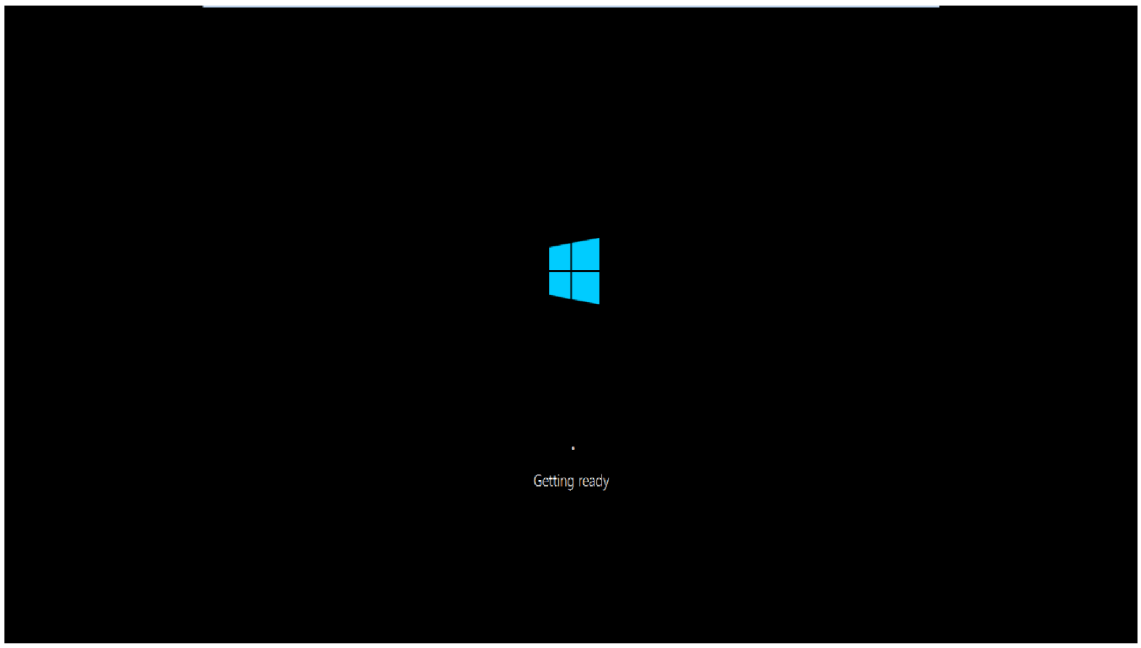


Dále zvolíme disk, na který chceme Windows nainstalovat, potvrdíme a počkáme, až se Windows nainstaluje.



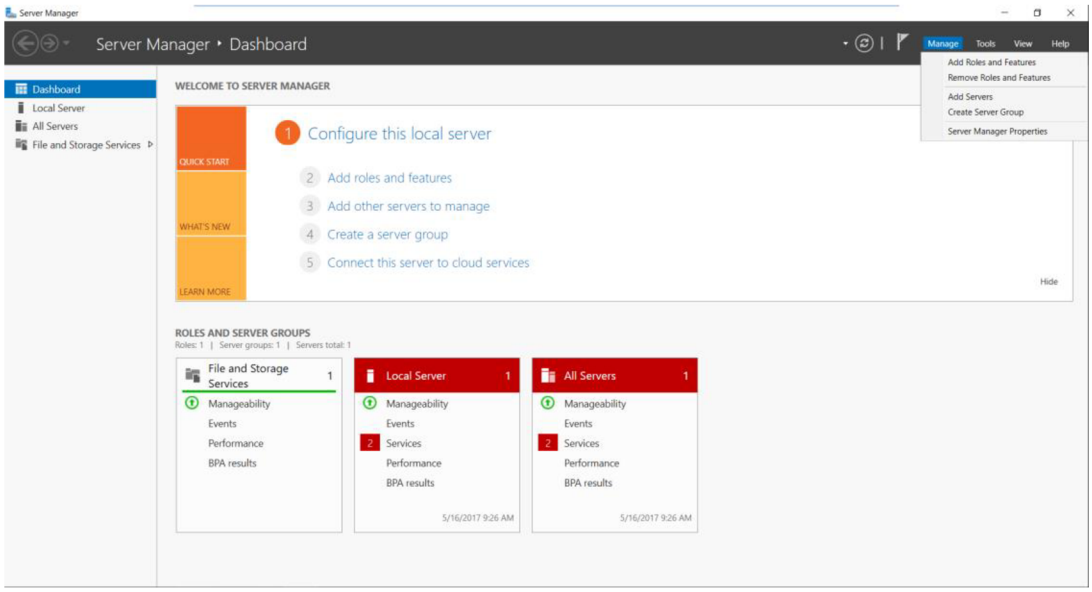


V této fázi už jen počkáme, až OS naběhne, a přihlásíme se.

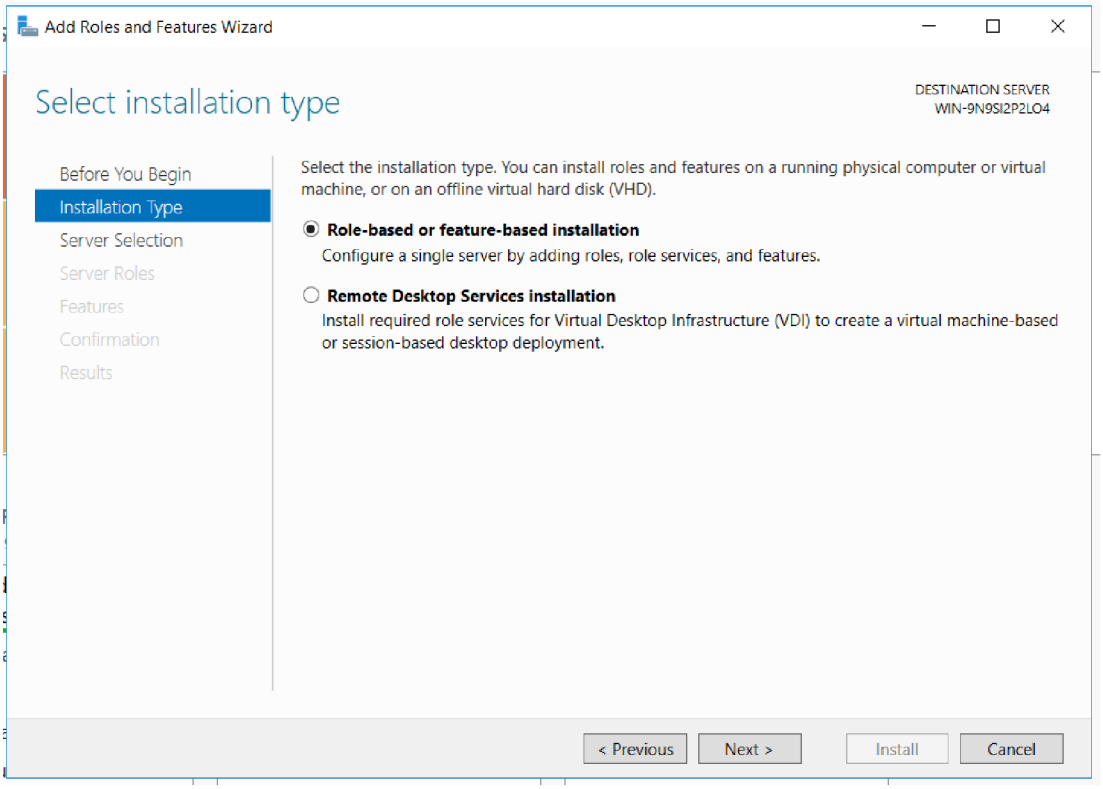


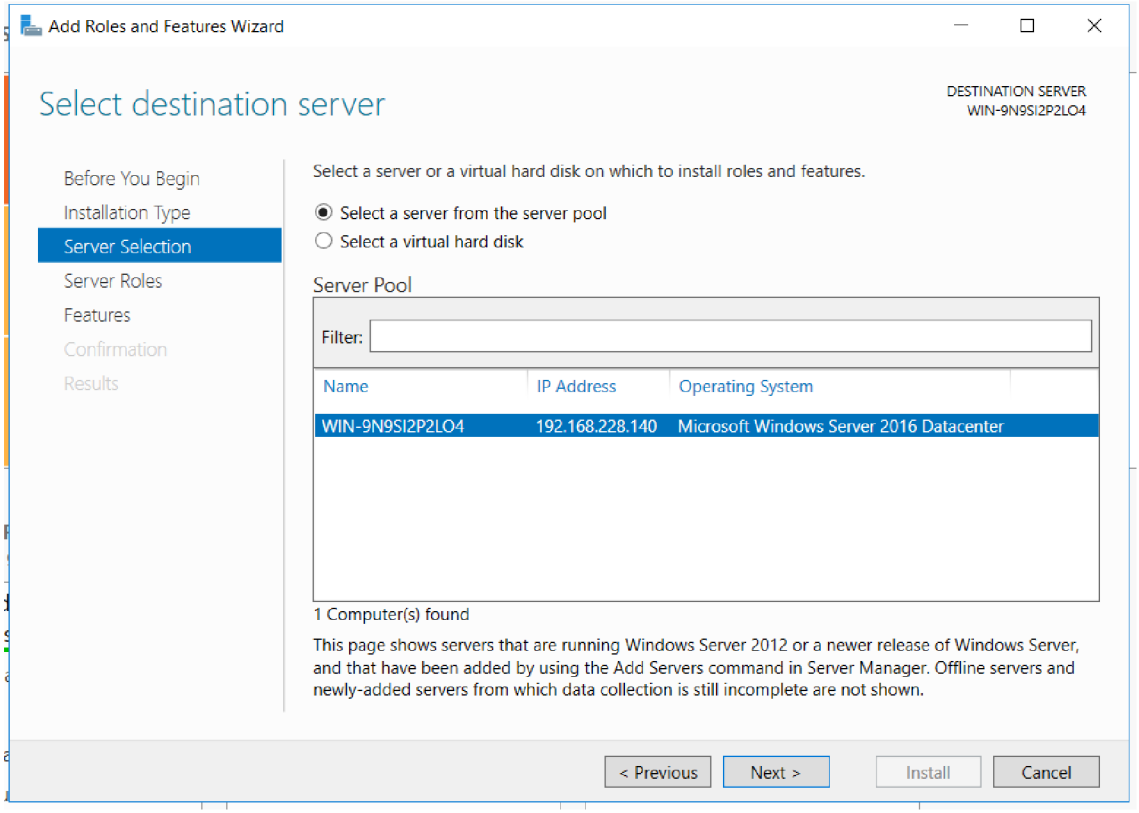
Příloha 2 - Instalace Active Directory Domain Services

AD DS nainstalujeme pomocí Server manageru – v pravém horním rohu najdeme Manage → Add Roles and Features.

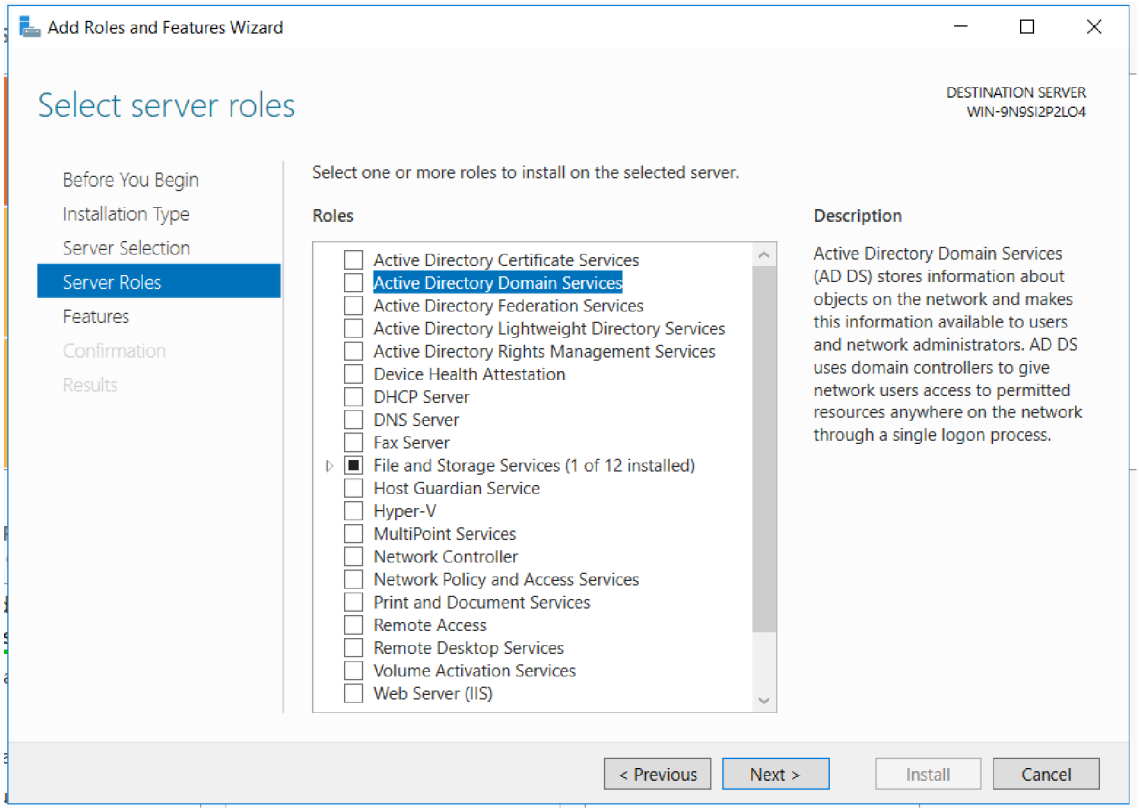


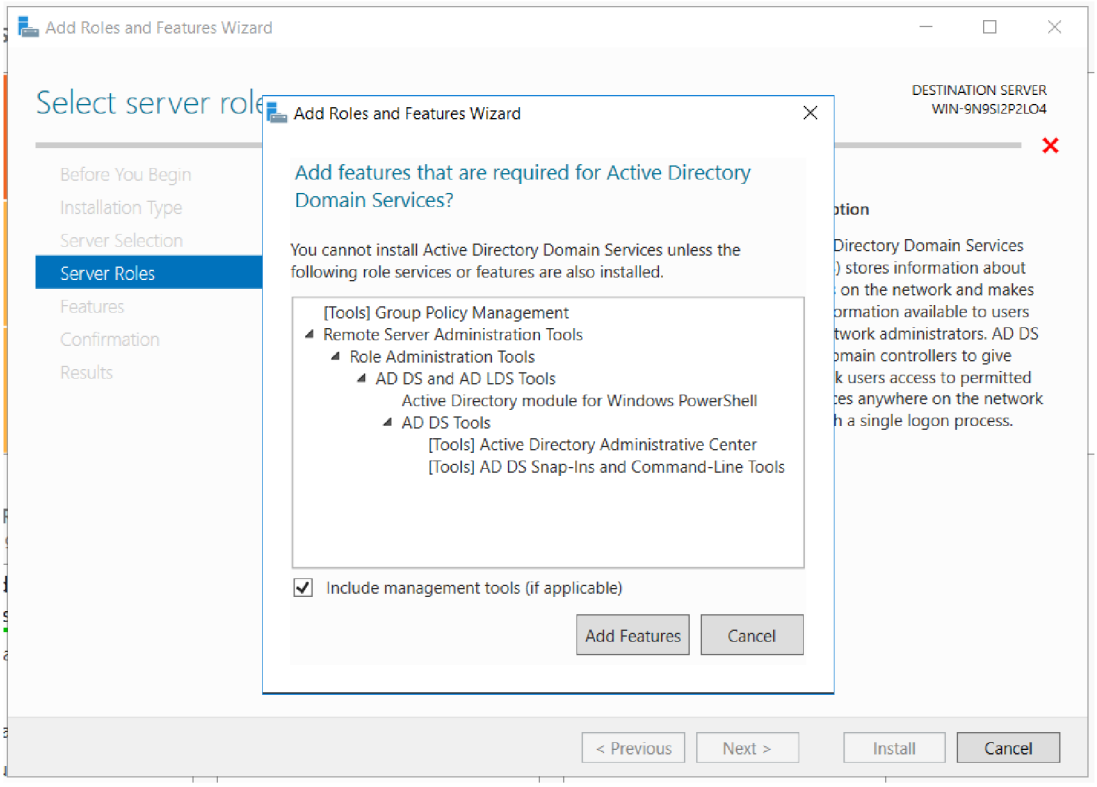
Naběhne průvodce, který nám s celou instalací pomůže.



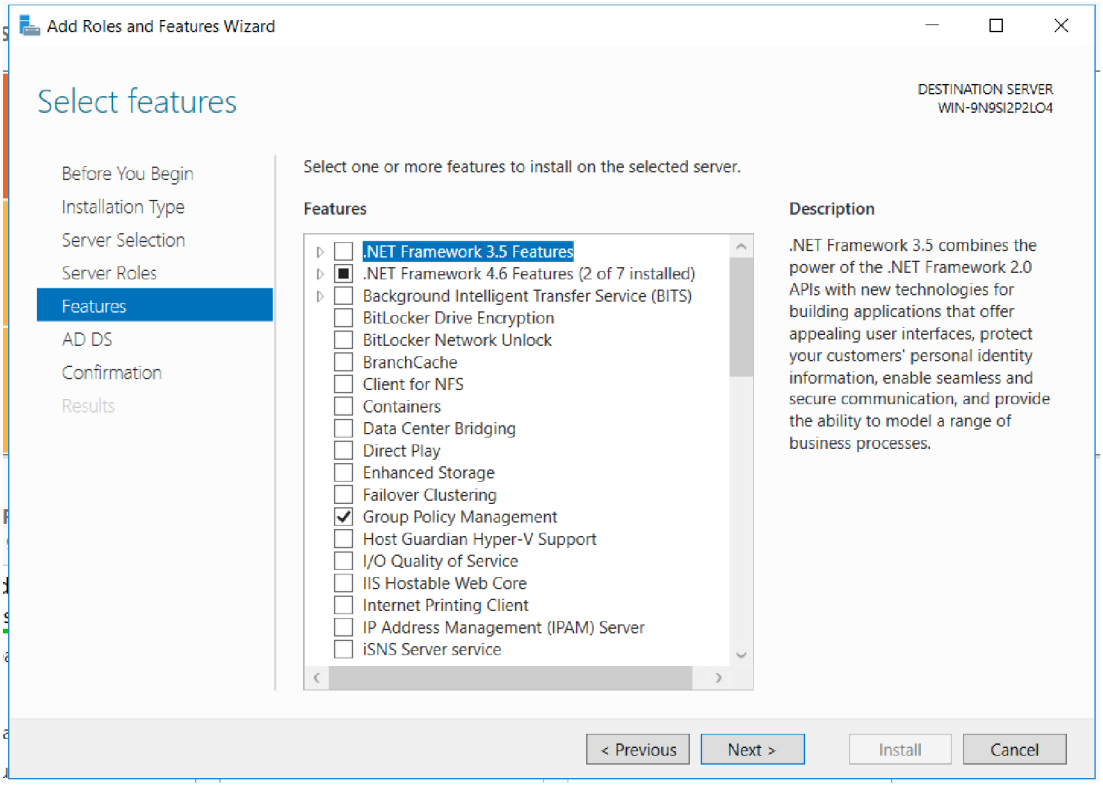


Zatrhneme „Active Directory Domain Services“ a klikneme na „Add features“.

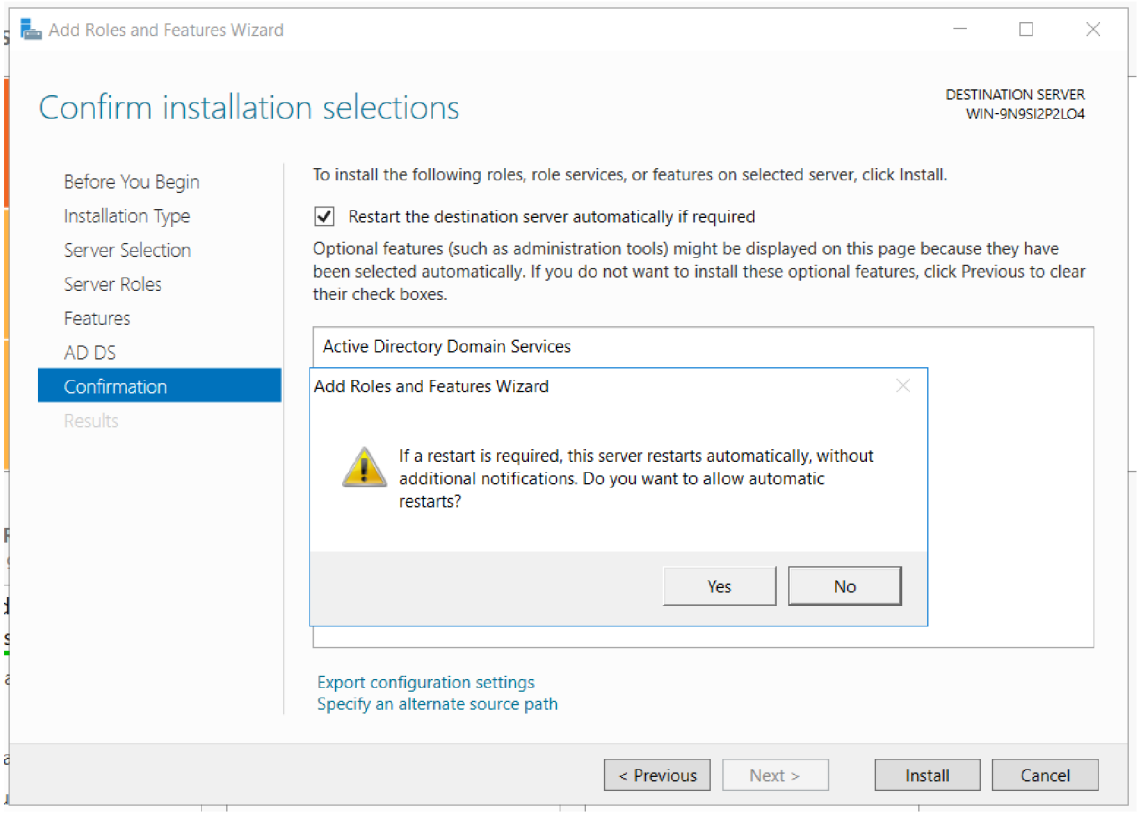


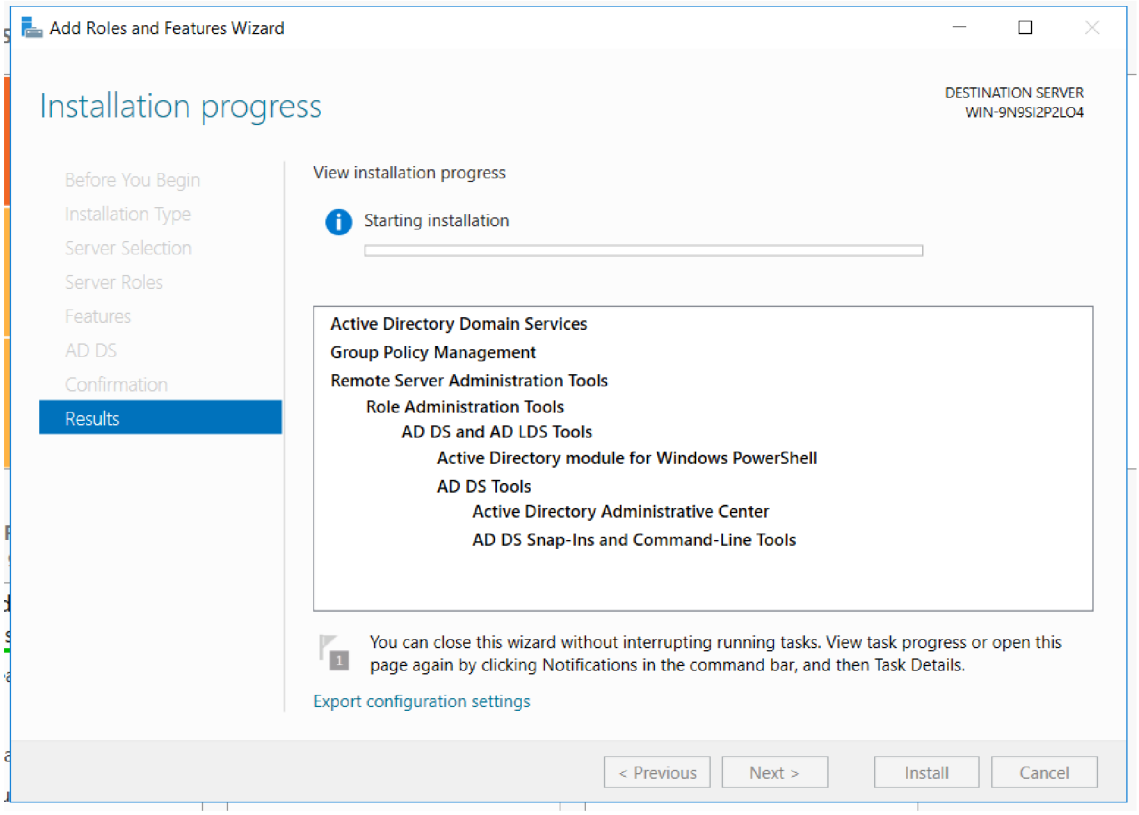


Tady můžeme vidět, že se nám do instalace automaticky zahrnul i Group Policy Management, který je spravován přes GPMC.



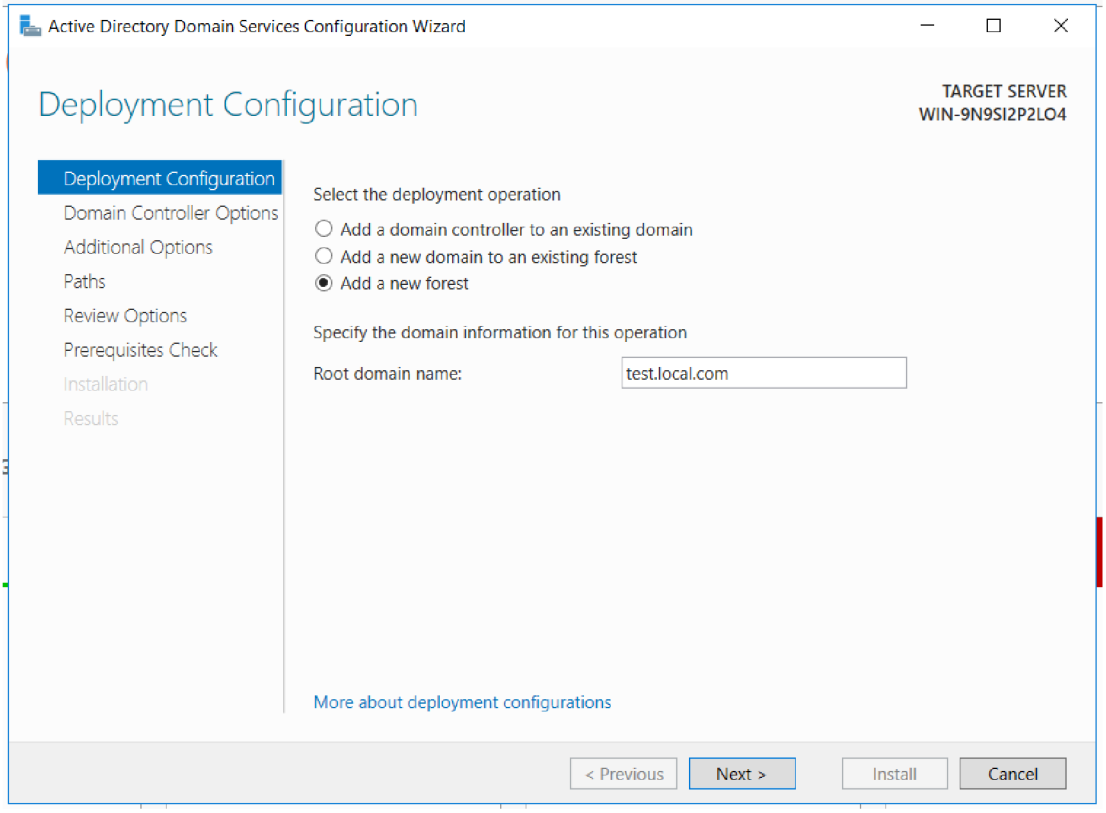
Už jen potvrdíme automatický restart a počkáme, až se doplněk AD DS nainstaluje.





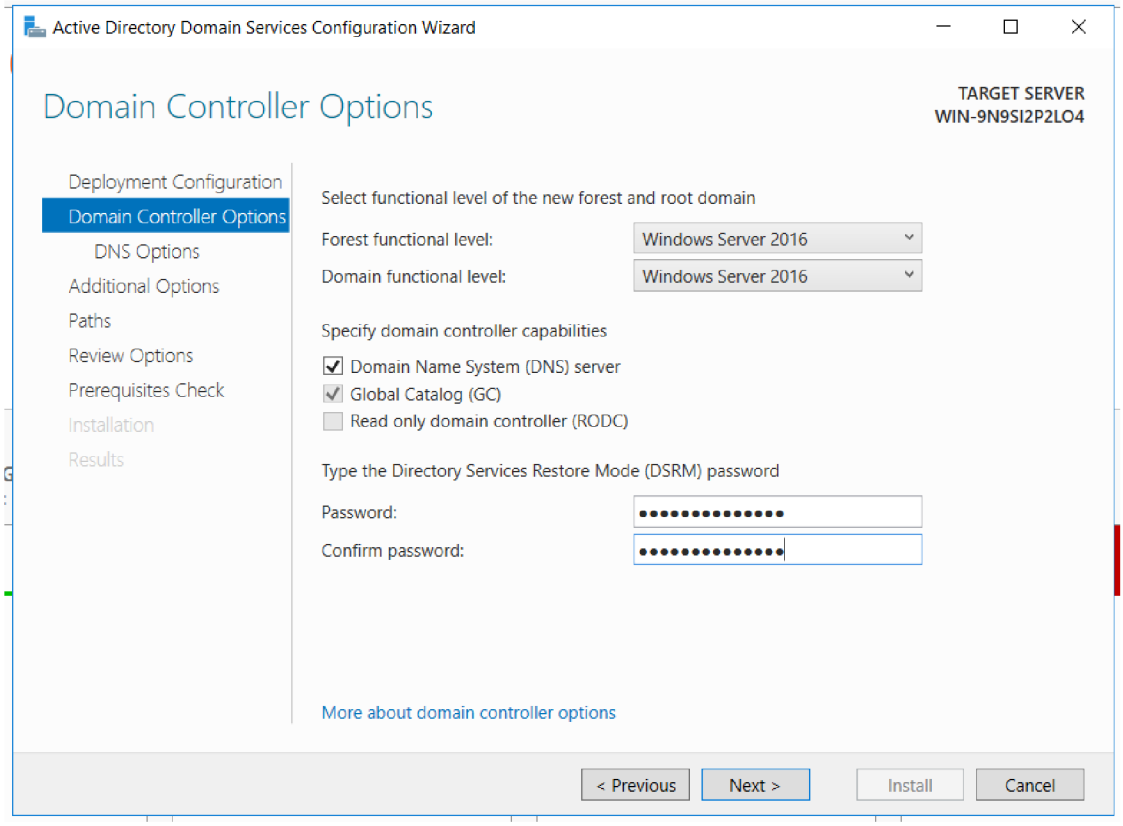
Po úspěšné instalaci AD DS budeme vyzváni ke konfiguraci domény a povýšení serveru na řadič domén.

Jelikož naše doména je testovací a potřebujeme prostředí oddělené od ostatních serverů, musíme založit nový forest.



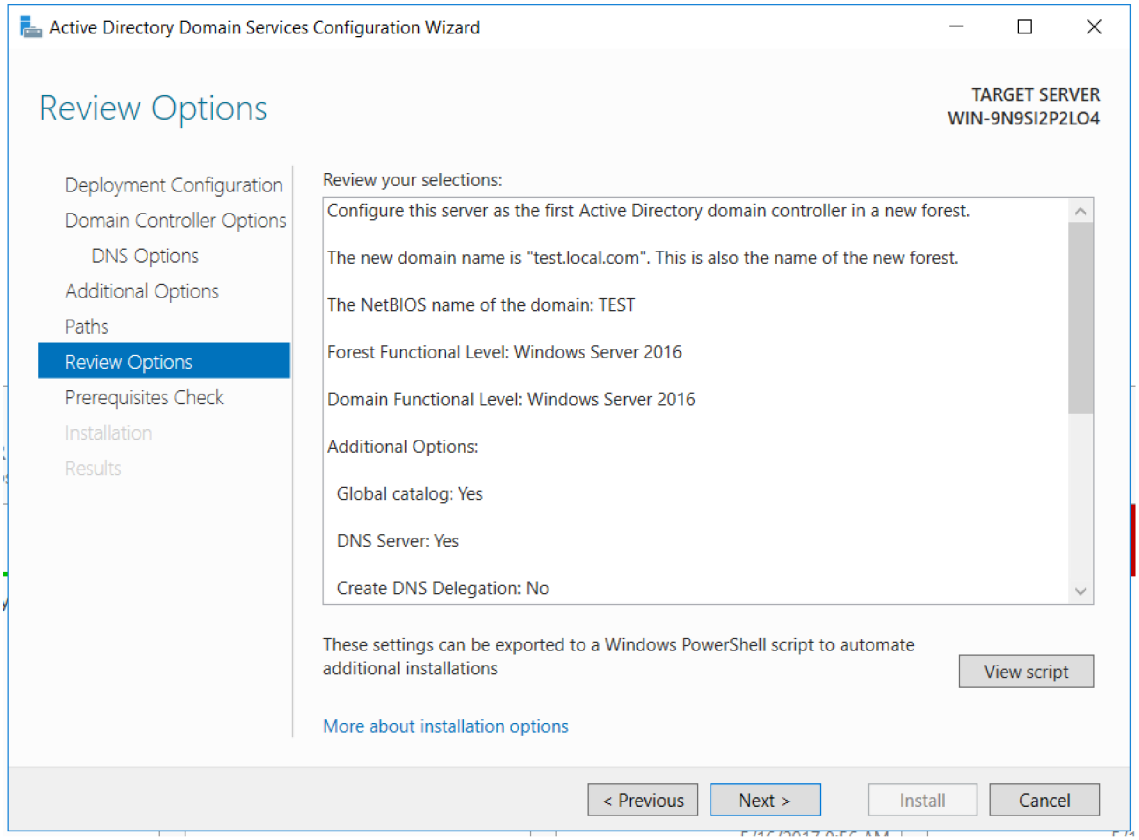
Dále zvolíme heslo pro DSRM – službu zajišťující obnovení a opravu domény, pokud je to potřeba.

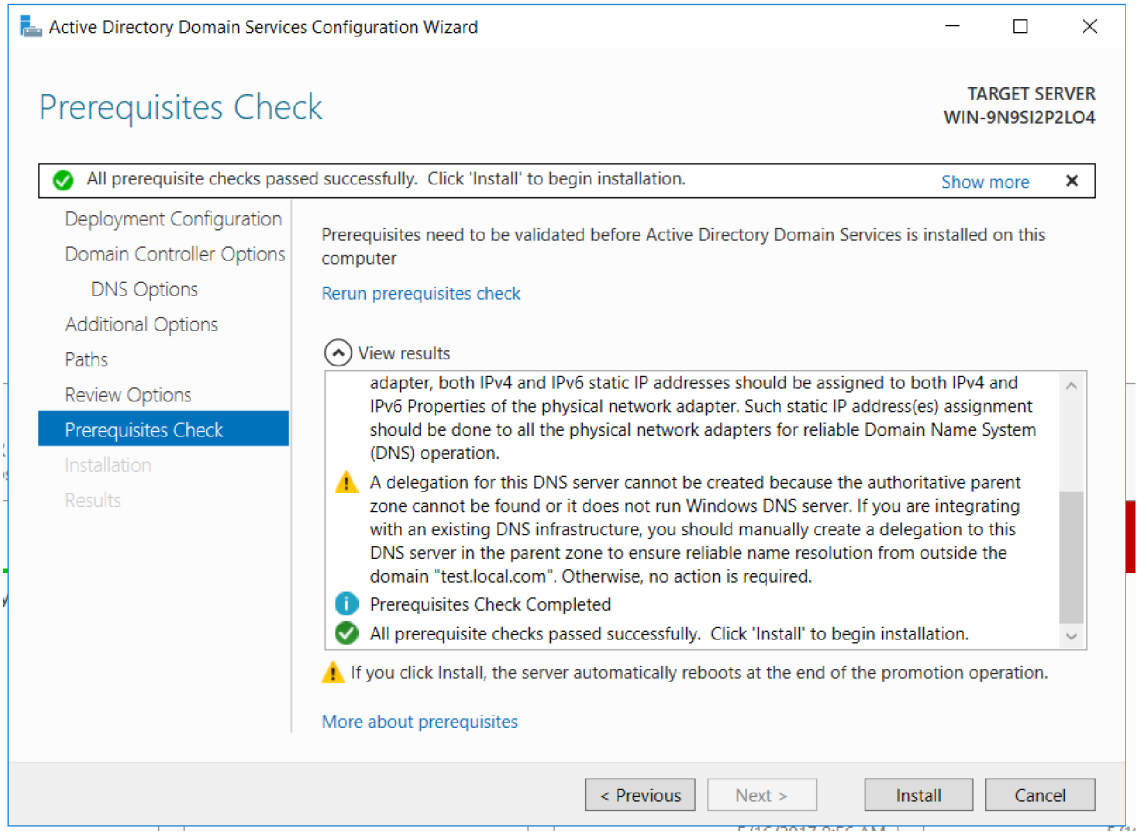
Součástí tohoto kroku je také konfigurace DNS serveru.



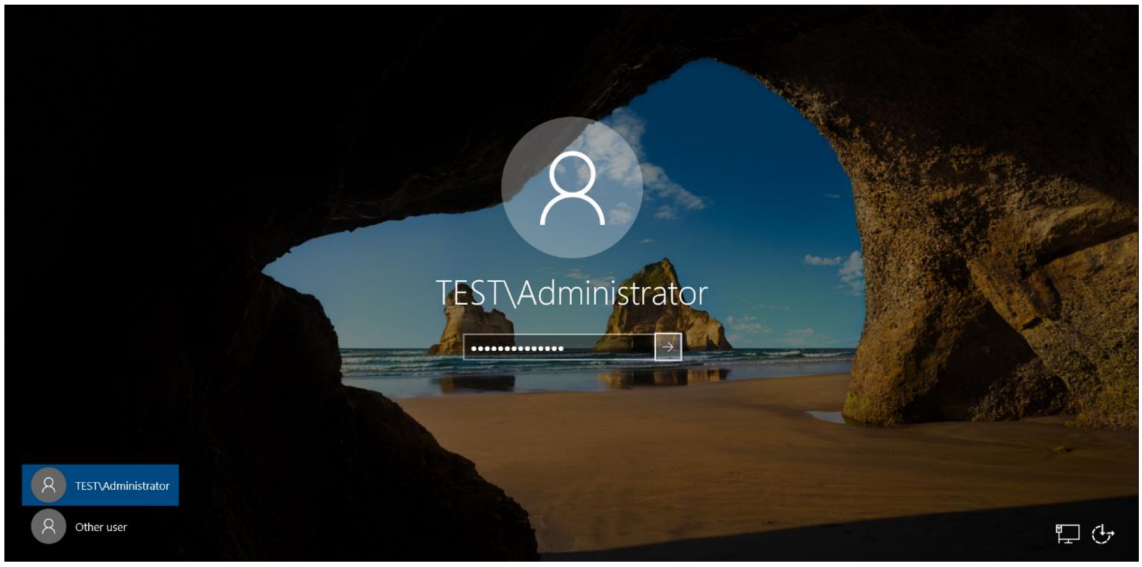
V dalších krocích se bude ověřovat námi vytvořené doménové jméno a konfigurovat cesty k log souborům.

Nakonec námi zvolené možnosti potvrdíme a nainstalujeme.


Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
WIN-9N9SI2P2LO4
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as the first Active Directory domain controller in a new forest.
The new domain name is "test.local.com". This is also the name of the new forest.
The NetBIOS name of the domain: TEST
Forest Functional Level: Windows Server 2016
Domain Functional Level: Windows Server 2016
Additional Options:
Global catalog: Yes
DNS Server: Yes
Create DNS Delegation: No
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel

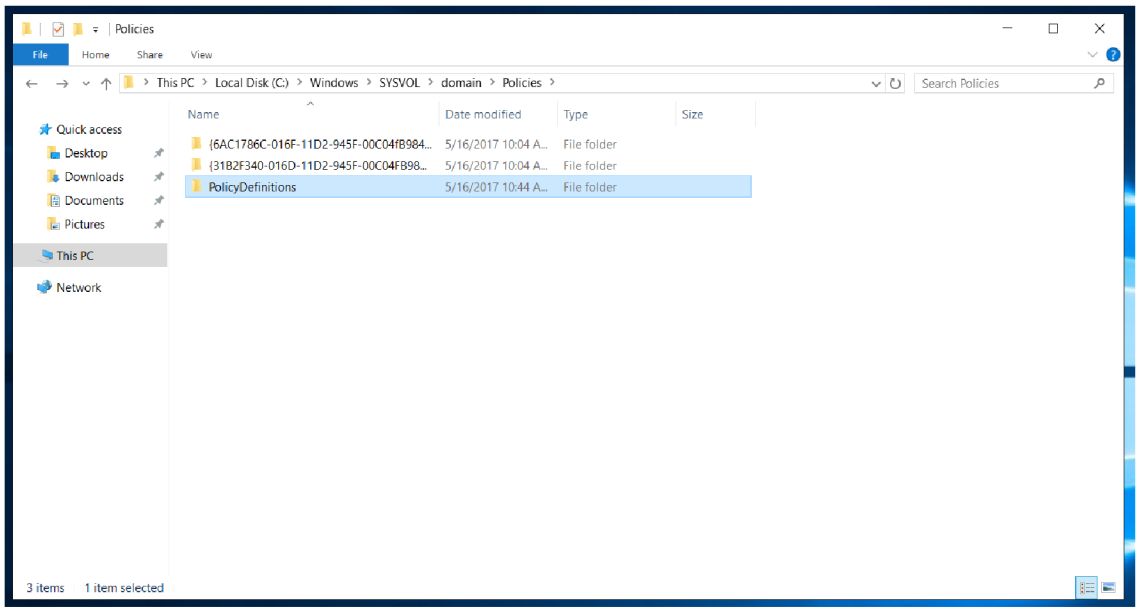

Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
WIN-9N9SI2P2LO4
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Rerun prerequisites check
View results
adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "test.local.com". Otherwise, no action is required.
Prerequisites Check Completed
All prerequisite checks passed successfully. Click 'Install' to begin installation.
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
< Previous
Next >
Install
Cancel

Pokud byla naše konfigurace úspěšná, server se restartuje a budeme se moci přihlásit pod doménovým účtem.

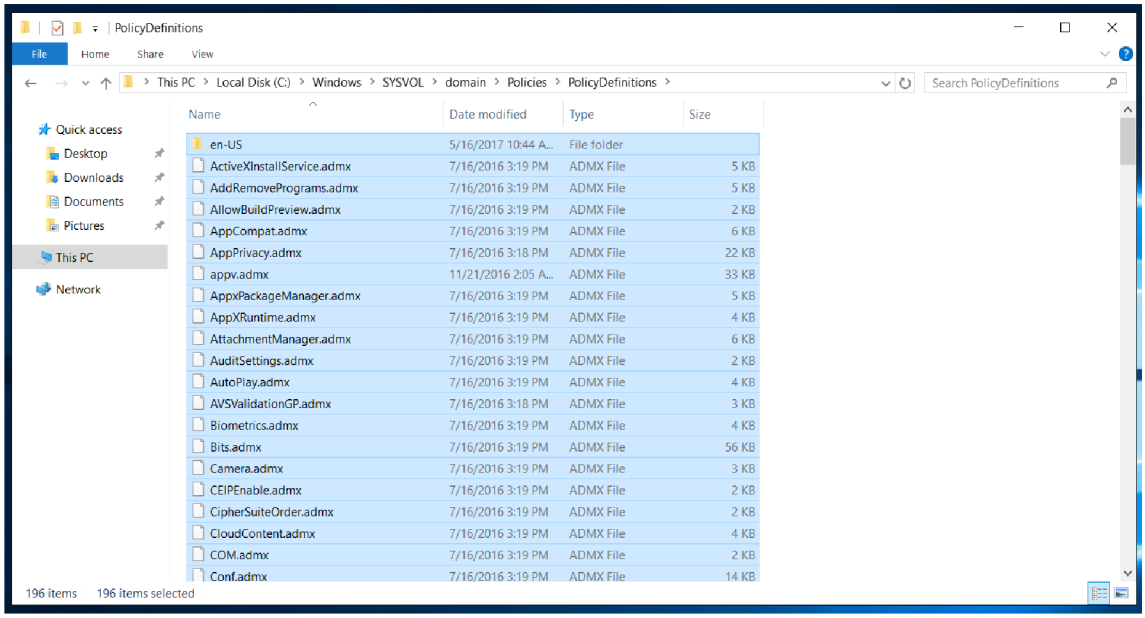


Příloha 3 - Vytvoření Central Store

Vytvoříme složku PolicyDefinitions v C:\Windows\SYSVOL\domain\Policies.



Do této složky rozbalíme námi stažené .admx a .adml šablony.



V případě, že se administrátor pokusí na členském serveru nebo jiném řadiči modifikovat nebo vytvořit politiku, podívá se tento server nejdříve na hlavní řadič domén, zda je na něm Central Store. Pokud jej najde, použije šablony z této složky.

Příloha 4 - Zobrazení MSS v Group Policy Editoru

Nejspolehlivějším způsobem, jak zobrazit MSS nastavení v Group Policy Editoru, je pomocí souboru sceregvl.inf

1. Přejděte do: %systemroot%\inf
2. Přes Vlastnosti→Zabezpečení→Pokročilé převezměte vlastnictví souboru sceregvl.inf
3. Otevřete sceregvl.inf
4. Sjeďte dolů k [Register Registry Values] a zadejte následující hodnoty:

;========= Start of MSS Registry Values =========

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon,1,%DisableAutoLogon%,0

MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\AutoReboot,4,%AutoReboot%,0

MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks,4,%AdminShares%,0

MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer,4,%AdminSharesServer%,0

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting,4,%DisableIPSourceRouting%,3,0|%DisableIPSourceRouting0%,1|%DisableIPSourceRouting1%,2|%DisableIPSourceRouting2%

MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters\DisableSavePassword,4,%DisableSavePassword%,0

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect,4,%EnableDeadGWDetect%,0

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect,4,%EnableICMPRedirect%,0

MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\Hidden,4,%HideFromBrowseList%,0

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime,4,%KeepAliveTime%,3,150000|%KeepAliveTime0%,300000|%KeepAliveTime1%,600000|%KeepAliveTime2%,1200000|%KeepAliveTime3%,2400000|%KeepAliveTime4%,3600000|%KeepAliveTime5%,7200000|%KeepAliveTime6%

MACHINE\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt,4,%NoDefaultExempt%,3,0|%NoDefaultExempt0%,1|%NoDefaultExempt1%,2|%NoDefaultExempt2%,3|%NoDefaultExempt3%

MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand,4,%NoNameReleaseOnDemand%,0

MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation,4,%NtfsDisable8dot3NameCreation%,3,0|%NtfsDisable8dot3NameCreation0%,1|%NtfsDisable8dot3NameCreation1%,2|%NtfsDisable8dot3NameCreation2%,3|%NtfsDisable8dot3NameCreation3%

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery,4,%PerformRouterDiscovery%,0

MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode,4,%SafeDllSearchMode%,0

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod,1,%ScreenSaverGracePeriod%,1

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect,4,%SynAttackProtect%,3,0|%SynAttackProtect0%,1|%SynAttackProtect1%

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions,4,%TcpMaxConnectResponseRetransmissions%,3,0|%TcpMaxConnectResponseRetransmissions0%,1|%TcpMaxConnectResponseRetransmissions1%,2|%TcpMaxConnectResponseRetransmissions2%,3|%TcpMaxConnectResponseRetransmissions3%

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions,4,%TcpMaxDataRetransmissions%,1

MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel,4,%WarningLevel%,3,50|%WarningLevel0%,60|%WarningLevel1%,70|%WarningLevel2%,80|%WarningLevel3%,90|%WarningLevel4%

MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\DisableIPSourceRouting,4,%DisableIPSourceRoutingIPv6%,3,0|%DisableIPSourceRouting0%,1|%DisableIPSourceRouting1%,2|%DisableIPSourceRouting2%

MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\TcpMaxDataRetransmissions ,4,%TcpMaxDataRetransmissionsIPv6%,1

;========= End of MSS Registry Values =========

5. Dále najděte položku [Strings] a zadejte následující hodnoty:

;========= Start of MSS Strings Values =========

DisableAutoLogon = "MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)"

AutoReboot = "MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)"

AdminShares = "MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure environments)"

AdminSharesServer = "MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secure environments)"

DisableIPSourceRouting = "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)"

DisableIPSourceRoutingIPv6 = "MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)"

DisableIPSourceRouting0 = "No additional protection, source routed packets are allowed"

DisableIPSourceRouting1 = "Medium, source routed packets ignored when IP forwarding is enabled"

DisableIPSourceRouting2 = "Highest protection, source routing is completely disabled"

DisableSavePassword = "MSS: (DisableSavePassword) Prevent the dial-up passsword from being saved (recommended)"

EnableDeadGWDetect = "MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)"

EnableICMPRedirect = "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes"

HideFromBrowseList = "MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)"

KeepAliveTime = "MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds"

KeepAliveTime0 ="150000 or 2.5 minutes"

KeepAliveTime1 ="300000 or 5 minutes (recommended)"

KeepAliveTime2 ="600000 or 10 minutes"

KeepAliveTime3 ="1200000 or 20 minutes"

KeepAliveTime4 ="2400000 or 40 minutes"

KeepAliveTime5 ="3600000 or 1 hour"

KeepAliveTime6 ="7200000 or 2 hours (default value)"

NoDefaultExempt = "MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic."

NoDefaultExempt0 = "Allow all exemptions (least secure)."

NoDefaultExempt1 = "Multicast, broadcast, & ISAKMP exempt (best for Windows XP)."

NoDefaultExempt2 = "RSVP, Kerberos, and ISAKMP are exempt."

NoDefaultExempt3 = "Only ISAKMP is exempt (recommended for Windows Server 2003)."

NoNameReleaseOnDemand = "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers"

NtfsDisable8dot3NameCreation = "MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames"

NtfsDisable8dot3NameCreation0 = "Enable 8Dot3 Creation on all Volumes"

NtfsDisable8dot3NameCreation1 = "Disable 8Dot3 Creation on all Volumes"

NtfsDisable8dot3NameCreation2 = "Set 8dot3 name creation per volume using FSUTIL (Windows 7 or later)

NtfsDisable8dot3NameCreation3 = "Disable 8Dot3 name creation on all volumes except system volume (Windows 7 or later)"

PerformRouterDiscovery = "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)"

SafeDllSearchMode = "MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)"

ScreenSaverGracePeriod = "MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)"

SynAttackProtect = "MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)"

SynAttackProtect0 = "No additional protection, use default settings"

SynAttackProtect1 = "Connections time out sooner if a SYN attack is detected"

TcpMaxConnectResponseRetransmissions = "MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged"

TcpMaxConnectResponseRetransmissions0 = "No retransmission, half-open connections dropped after 3 seconds"

TcpMaxConnectResponseRetransmissions1 = "3 seconds, half-open connections dropped after 9 seconds"

TcpMaxConnectResponseRetransmissions2 = "3 & 6 seconds, half-open connections dropped after 21 seconds"

TcpMaxConnectResponseRetransmissions3 = "3, 6, & 9 seconds, half-open connections dropped after 45 seconds"

TcpMaxDataRetransmissions = "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)"

TcpMaxDataRetransmissionsIPv6 = "MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)"

WarningLevel = "MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning"

WarningLevel0 = "50%"

WarningLevel1 = "60%"

WarningLevel2 = "70%"

WarningLevel3 = "80%"

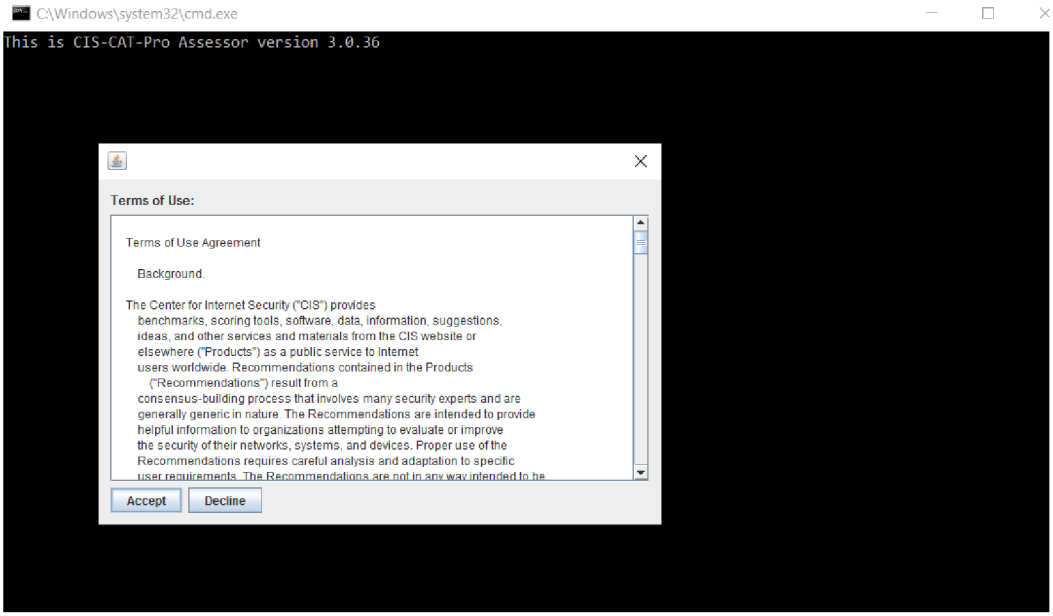
WarningLevel4 = "90%"

;========= End of MSS Strings Values =========

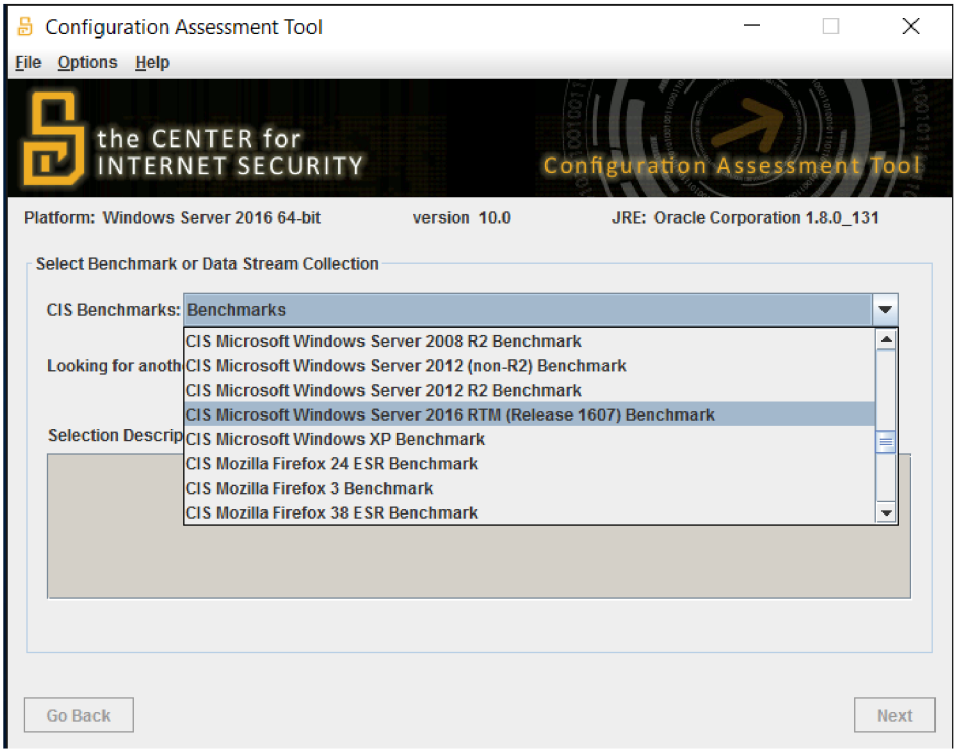
6. Uložte sceregvl.inf
7. V příkazovém řádku spusťte: **regsvr32 scecli.dll**
8. MSS politiky jsou nyní vidět v Group Policy Editoru ve větvi Security Settings.

Příloha 5 - Kontrola nastavení pomocí programu CIS-CAT

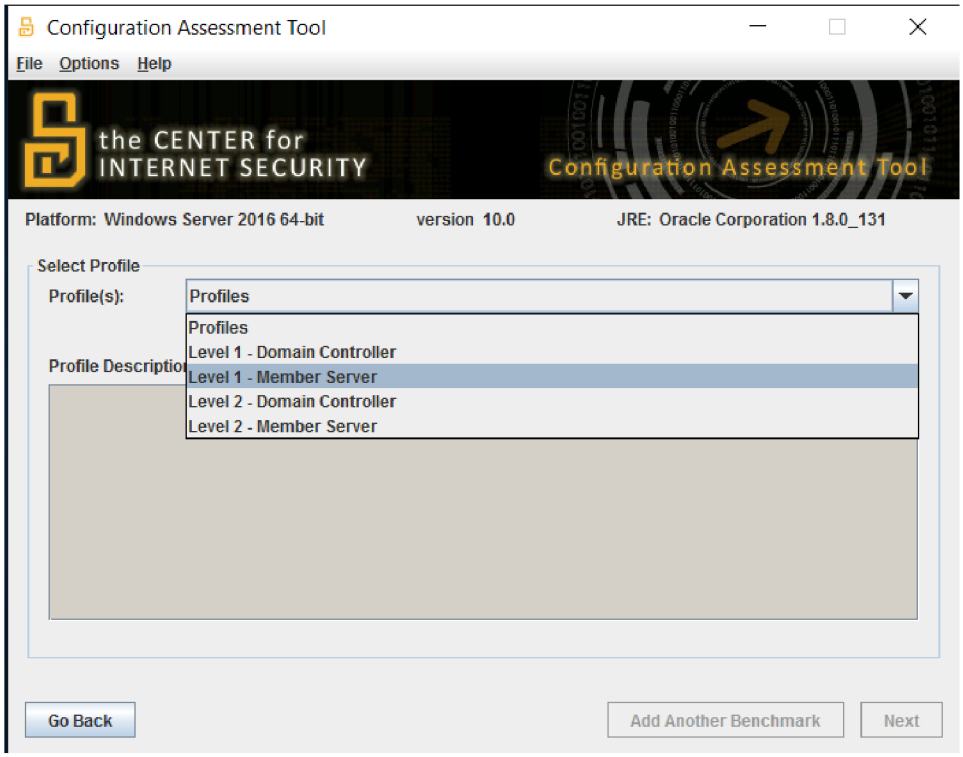
Prvním krokem po spuštění programu je přijetí licenčních podmínek.



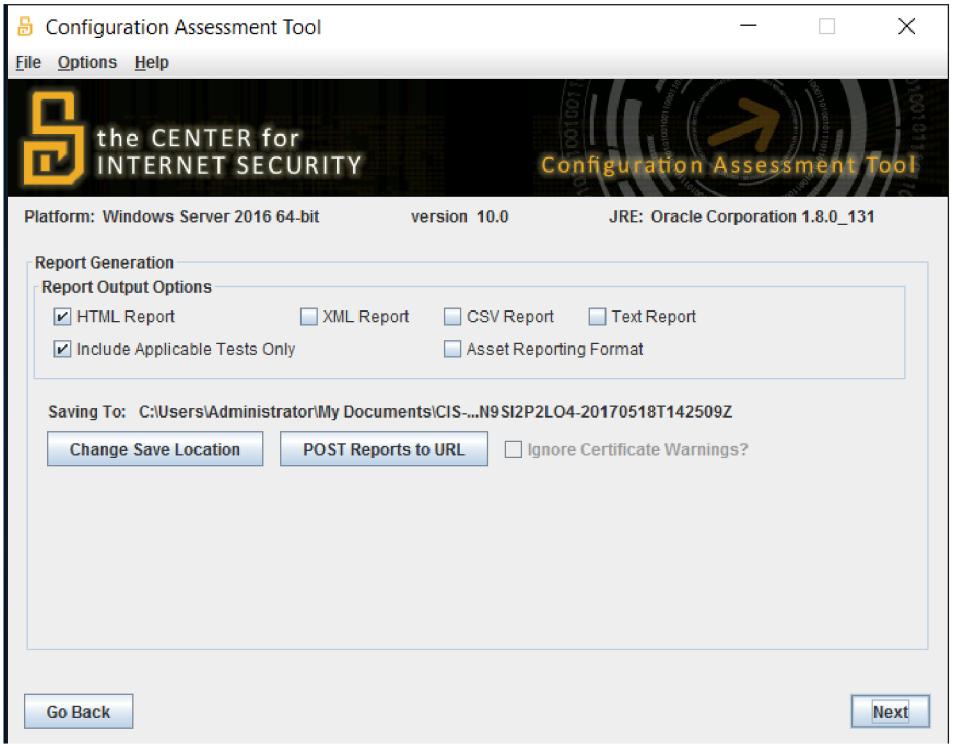
Dále vybereme verzi benchmarku. Musíme zvolit benchmark shodný s posuzovaným systémem, jinak vyskočí chyba.



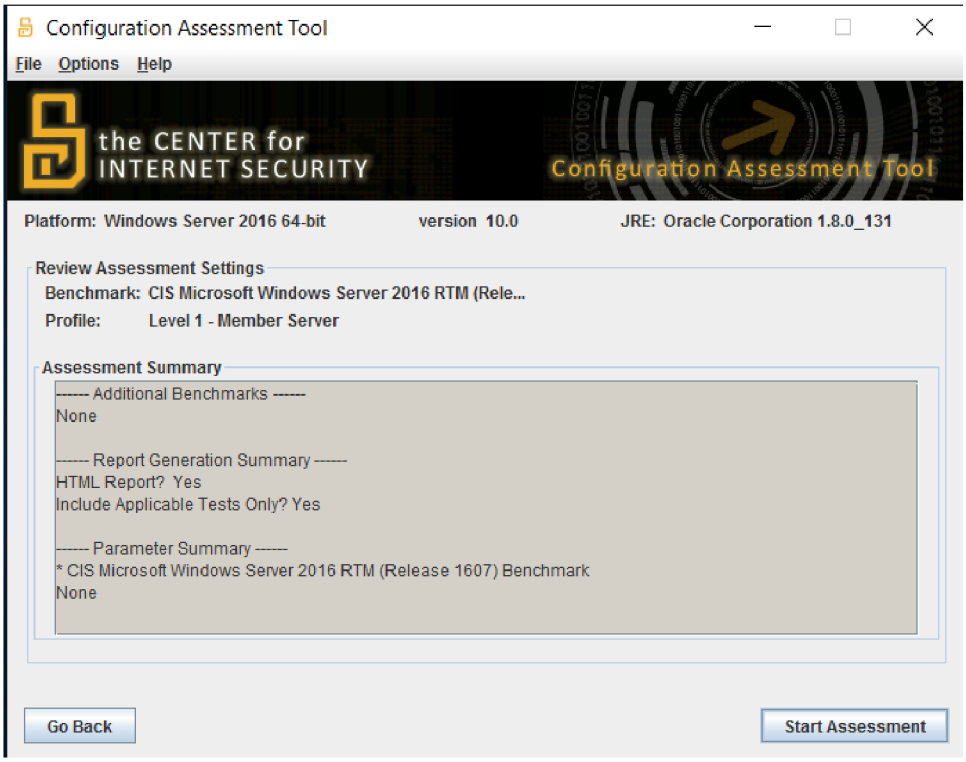
Podle posuzovaného systému vybereme profil.



V dalším kroku zvolíme, v jakých formátech chceme výslednou zprávu.



Kliknutím na Start Assessment začneme kontrolu.



Teď už jen počkáme, až kontrola proběhne a vygenerují se reporty.