Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Zlepšování služeb pro koncové uživatele pomocí nástroje Identity manager

Martin TOMAN

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Martin Toman

Informatika

Název práce

Zlepšování služeb pro koncové uživatele pomocí nástroje Identity Manager

Název anglicky

Improving Services for End Users Using a Tool Identity Manager

---

Cíle práce

Cílem diplomové práce je návrh implementace nástroje Identity Manager. Implementace představuje usnadnění práce s identitami a zvýšení uživatelského komfortu.

Dílčí cíle:
- přehled řešené problematiky
- analýza současného stavu
- návrh strategie řešení
- předběžné vyčíslení nákladů
- testování, zhodnocení
- uvedení závěrů a doporučení

Metodika

Práce se skládá ze dvou částí. V první části je zpracován přehled řešené problematiky s důrazem na Identity Management. Nejprve je představen nástroj Microsoft Identity Manager, který je následně porovnán s nástroji konkurenčních firem.

V druhé části je provedena analýza servisních požadavků pro odhalení opakujících se problémů s účty, kterým je potřeba předcházet. Dále je uvedena tvorba virtuálního laboratorního prostředí, které simuluje skutečnou firemní infrastrukturu. Do něj je implementován vybraný nástroj, ve kterém jsou nastaveny funkce pro usnadnění práce s identitami a zvýšení uživatelského komfortu. Aplikace je podrobena kvalitativnímu a kvantitativnímu šetření. Na základě výsledků šetření je provedeno zhodnocení a doporučení dalšího postupu.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

Uživatel, účet, administrátor, identita, Identity Manager, Active Directory, Windows, Linet

---

Doporučené zdroje informací

Daniel, RUEST, Nelson. Virtualizace – Podrobný průvodce.: Computer Press, a.s., 2010. ISBN 978-80-251-2676-9

ITIL V3 Foundation Handbook – Pocketbook from the Official Publisher of ITIL.: The Stationery Office, 2009. ISBN 978-01-133-1197-2

KELBLEY, John. Hyper-V – Podrobný průvodce administrátora.: Computer Press, a.s., 2009. ISBN 978-80-251-3286-9

STANEK, William. Active Directory – Kapesní rádce administrátora.: Computer Press, a.s., 2009. ISBN 978-80-251-2555-7

STANEK, William. Windows Server 2003 – Kapesní rádce administrátora.: Computer Press, a.s., 2007. ISBN 978-80-251-1654-9

STEADMAN, David. Microsoft Identity Manager 2016 Handbook.: Packt Publishing, 2016. ISBN 978-17-852-8392-5.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 12. 6. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 12. 01. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „Zlepšování služeb pro koncové uživatele pomocí nástroje Identity manager" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29. 3. 2019 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D. za odborné vedení mé práce a Bc. Petru Němečkovi za vytvoření vhodných podmínek pro vznik této práce.

Zlepšování služeb pro koncové uživatele pomocí nástroje Identity Manager

Abstrakt

Hlavní náplní práce je návrh implementace a následné testování vybraných nástrojů pro usnadnění práce s identitami a zvýšení uživatelského komfortu. V teoretické části jsou vysvětleny pojmy, které jsou použity v práci, představeny současné procesy řízení účtů a navrženy nové, efektivnější procesy. Dále jsou porovnány dostupné nástroje pro řízení uživatelských účtů od různých společností. Podniková síť využívá především produkty společnosti Microsoft, proto byly zvoleny nástroje od této společnosti: „Microsoft Azure Active Directory“ a „Microsoft Identity Manager“.

V praktické části je provedena analýza pro odhalení konkrétních nedostatků, které je potřeba zlepšit, následně je uvedena simulace firemní infrastruktury ve virtuálním testovacím prostředí „Hyper-V“, do které jsou implementovány oba vybrané nástroje a nastaveny potřebné funkce. Usnadnění práce s identitami bylo dosaženo napojením databáze uživatelů na databázi personálního oddělení, čímž byla zvýšena rychlost tvorby nového účtu a zajištěna integrita dat. Uživatelský komfort byl zvýšen nastavením funkce pro samoobslužný reset hesla. Obě funkce nabízí nástroj „Microsoft Identity Manager“, produkt „Microsoft Azure Active Directory“ se ukázal jako nevhodný. Následuje doporučení dalšího postupu a finanční analýza.

Klíčová slova: Uživatel, účet, administrátor, identita, Identity Manager, Active Directory, Microsoft, Windows, Linet

Improving Services for End Users Using a Tool Identity Manager

Abstract

The main task of the thesis is the design of implementation and subsequent testing of selected tools to facilitate work with identities and increase user comfort. The theoretical part explains the terms that are used in the work, presents the current processes of account management and proposes new, more efficient processes. Furthermore, the available tools for managing user accounts from different companies are compared. The corporate network uses primarily Microsoft products, therefore tools from this company have been selected: "Microsoft Azure Active Directory" and "Microsoft Identity Manager".

In the practical part there is an analysis for the detection of specific shortcomings that need to be improved, followed by a simulation of the company infrastructure in the virtual testing environment "Hyper-V", into which both selected tools are implemented, and necessary functions are set. Identity facilitation has been achieved by linking the user database to the HR department database to increase the speed of new account creation and ensure data integrity. User comfort has been enhanced by setting the self-service password reset feature. Both features are offered by the "Microsoft Identity Manager" tool, "Microsoft Azure Active Directory" has proven to be inappropriate. Following is a recommendation for further actions and financial analysis.

Keywords: User, Account, Administrator, Identity, Identity Manager, Active Directory, Microsoft, Windows, Linet

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AD – Aktivní adresář (Active Directory)

DC – Doménový řadič (Domain Controller)

HR – Lidské zdroje (Human Resources)

IT – Informační technologie

LG – Linet-group

MPR – Management Policy Rules

MIM – Microsoft Identity Manager

OU – Organizační jednotka (Organizational Unit)

SLA – Dohoda o úrovni služeb (Service Level Agreement)

1 Úvod

Autor této práce vede tým IT odborníků, který je zodpovědný za řešení uživatelských požadavků a problémů ve firmě LINET spol. s r.o. Společnost se potýká s problémem, kterým je nedostatečné řízení uživatelských účtů a přístupů do informačních systémů. Bez efektivního řízení se zvyšuje riziko napadení firmy při ponechání aktivního účtu po odchodu zaměstnance, nebo při ponechání nepotřebných práv po změně pozice, a zvyšují se náklady při prodlevě mezi nástupem nového zaměstnance a vytvořením účtu s potřebnými přístupovými právy.

Dalším zjištěným nedostatkem jsou hesla uživatelů s neomezenou platností. Před nastavením expirace hesel pro zvýšení zabezpečení je nutné zajistit, aby uživatelé měli možnost si samoobslužně resetovat zapomenuté heslo. Proto jsou v této práci nalezeny vhodné nástroje, které mohou současný stav zlepšit. Tyto nástroje jsou implementovány do virtuálního testovacího prostředí, které simuluje reálnou síťovou infrastrukturu firmy. Jednotlivá řešení jsou otestována, zhodnocena a firmě je doporučen další postup. Poté je provedena finanční analýza, vyčísleny náklady na implementaci a odhadnuty úspory.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem diplomové práce je návrh implementace nástroje Identity Manager. Implementace představuje usnadnění práce s identitami a zvýšení uživatelského komfortu.

Dílčí cíle:

- přehled řešené problematiky
- analýza současného stavu
- návrh strategie řešení
- testování, zhodnocení
- předběžné vyčíslení nákladů
- uvedení závěrů a doporučení

2.2 Metodika

Práce se skládá ze dvou částí. V první části je zpracován přehled řešené problematiky s důrazem na Identity Management. Nejprve je představen nástroj Microsoft Identity Manager, který je následně porovnán s nástroji konkurenčních firem.

V druhé části je provedena analýza servisních požadavků pro odhalení opakujících se problémů s účty, kterým je potřeba předcházet. Dále je uvedena tvorba virtuálního laboratorního prostředí, které simuluje skutečnou firemní infrastrukturu. Do něj je implementován vybraný nástroj, ve kterém jsou nastaveny funkce pro usnadnění práce s identitami a zvýšení uživatelského komfortu. Aplikace je podrobena kvalitativnímu a kvantitativnímu šetření. Na základě výsledků šetření je provedeno zhodnocení a doporučení dalšího postupu.

3 Teoretická východiska

V teoretické části jsou vymezeny pojmy, které jsou později používány v praktické části této práce, a porovnány vybrané nástroje pro řízení identit.

3.1 Entita a identita

Systém, který slouží pro řízení identit je založen na práci s identitami, které představují reálné entity. Ty jsou přímými, či nepřímými účastníky celého systému. Nejprve je tedy třeba definovat entitu a identitu.

3.1.1 Entita

„Entitu je možné definovat jako věc schopnou samostatné existence, kterou lze jednoznačně identifikovat. Entita v informatice je jakýkoliv objekt reálného světa, který je zachycen v datovém modelu. Může to být například osoba, zařízení, či skupina práv. Entita musí být jedinečná, musí tedy být možné ji odlišit od ostatních entit a musí existovat nezávisle na nich“. [1]

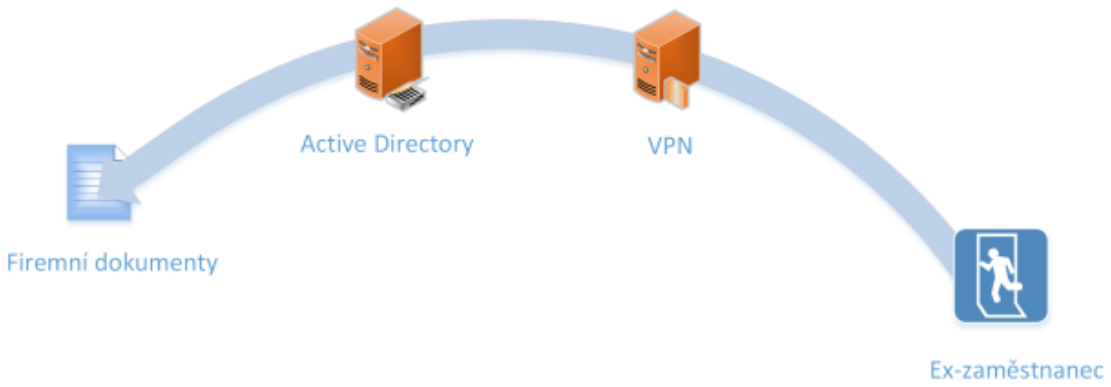
3.1.2 Identita

„Identita je shoda (stejnost) zásadních a charakteristických vlastností (atributů) neměnících se v čase a prostoru. Je nutné připomenout, že identita entity se může týkat jak osoby (fyzické, právnické), tak i věci (např. počítače, aplikace nebo jejich částí)“. [2] „Identita je něco, co lze ověřit (autentizace) a na základě ověření může proces pokračovat. Identitu lze zfalšovat, pak se nazývá „falešná identita“. Řízení a správa identit se nazývá Identity management“. [3]

3.2 Řízení identit

„Identity management je oblast, která se zabývá řízením a správou identit. Laicky řečeno se stará o to, aby každý člověk ve společnosti měl k dispozici ty přístupy do systémů, které má mít, a to tehdy, kdy je má mít. A také, aby měl přístup jen k těm datům, která

spadají do jeho kompetence. Řečeno slovy informační bezpečnosti, aby byla dodržena důvěrnost, integrita a dostupnost informací“. [4]



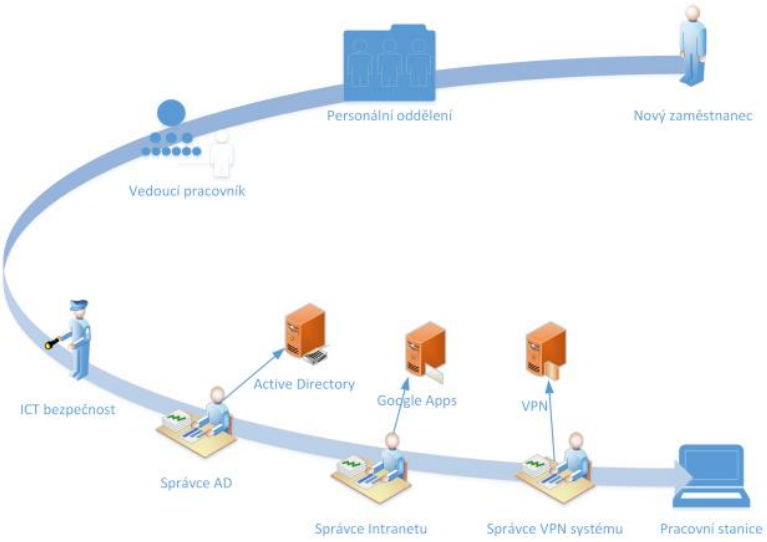
Obrázek 1 - Únik dat pomocí spícího účtu [4]

V případě, že by uživatel měl přístup k citlivým datům v nesprávnou chvíli (například po vyhození z firmy) může dojít k odcizení dat, odprodání konkurenci a následné ztrátě většiny zákazníků, což může vést až k zániku celé firmy. Z těchto důvodů je třeba ošetřit, aby ve větších firmách (hranice je přibližně 50 zaměstnanců), každý přistupoval pouze tam, kam to vyžaduje jeho pracovní zařazení. Existují dva možné přístupy řízení identit: metodický a technický.

3.2.1 Metodický přístup

V metodickém případě jsou stanoveny postupy, jak identity a oprávnění přidělovat, měnit, odebírat a ty jsou přiřazeny lidem v organizačním schématu. Proces je doplněn o formuláře a evidenční tabulky a způsoby, jak získat reporty pro bezpečnost. Jsou určeni správci odpovědní za jednotlivé informační systémy. [4]

3.2.1.1 Nástup nového zaměstnance

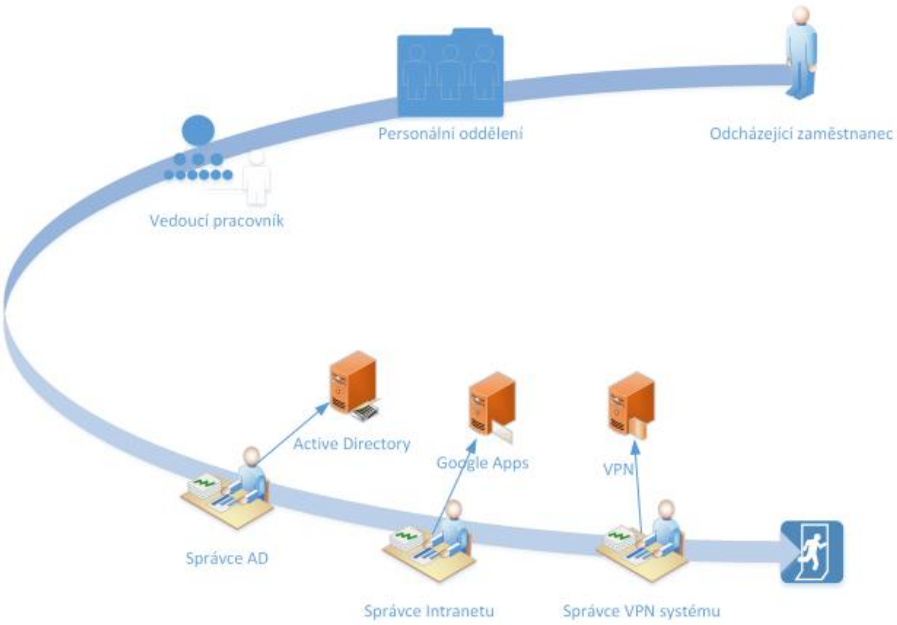


Obrázek 2 - Nástup nového zaměstnance v metodickém přístupu [4]

Nový zaměstnanec nejprve navštíví personální oddělení, kde dostane seznam přístupů, které pro svou pozici bude potřebovat. Jeho vedoucí pracovník seznam zkontroluje a případně doplní. Poté je seznam prověřen z hlediska ICT bezpečnosti a zaměstnanec se seznamem navštíví správce jednotlivých informačních systémů, aby mu požadované přístupy přidělili. Po udělení přístupů může začít pracovat. Tento postup je časově náročný, plné zapojení zaměstnance může trvat i několik dní.

Problém nastává u aktualizace informací, například při změně pozice pracovníka. Rychlost a kvalita předání informací z jednoho systému do druhého záleží na míře integrace těchto systémů. „Někde je možno využít společný zdroj dat (Active Directory, databázi), jinde je třeba vytvořit dvojbodové spojení mezi systémy (peer-to-peer) nebo se spolehnout na e-mailové, či ústní předání“ [4]

3.2.1.2 **Odchod zaměstnance**



Obrázek 3 - Odchod zaměstnance v metodickém přístupu [4]

Při odchodu zaměstnance z firmy mu personální oddělení přidělí výstupní list [Příloha I]. V tom jsou předepsána jednotlivá oddělení, které zaměstnanec musí obejít a získat podpis odpovědného pracovníka, který stvrzuje vyrovnání případných závazků se společností.

Pro získání podpisu za IT oddělení slouží další formulář „Odchod zaměstnance“ [Příloha II], ve kterém jsou vyplněné veškeré informační systémy, do kterých mohl mít uživatel přístup. Zaměstnanec si musí domluvit přesný termín s kompetentní osobu za IT, která mu zakáže přístup do klíčových informačních a souborových systémů. Úprava každého z přístupů je zanesena do formuláře. Po ošetření hlavních přístupů je výstupní list zaměstnance [Příloha I] podepsán vedoucím IT, nebo jeho zástupcem. Částečně vyplněný formulář „Odchod zaměstnance“ [Příloha II] je oskenován do servisního požadavku, který je následně předáván na správce ostatních systémů, kteří přístup ověří, případně zruší a požadavek předají dále.

Tento proces je silně navázán na evidenci o zaměstnancích v personálním oddělení. V případě, že zaměstnanec změní svou pracovní pozici, je právě personální oddělení povinné zajistit, aby již neměl přístup do systémů, které v nové pozici nevyužije. Nebo v případě, kdy zaměstnanec neprovede výstupní proces s výstupním listem, bez účasti personálního oddělení se správci informačních systémů nedozví o tom, že již zaměstnanec ve firmě nepracuje.

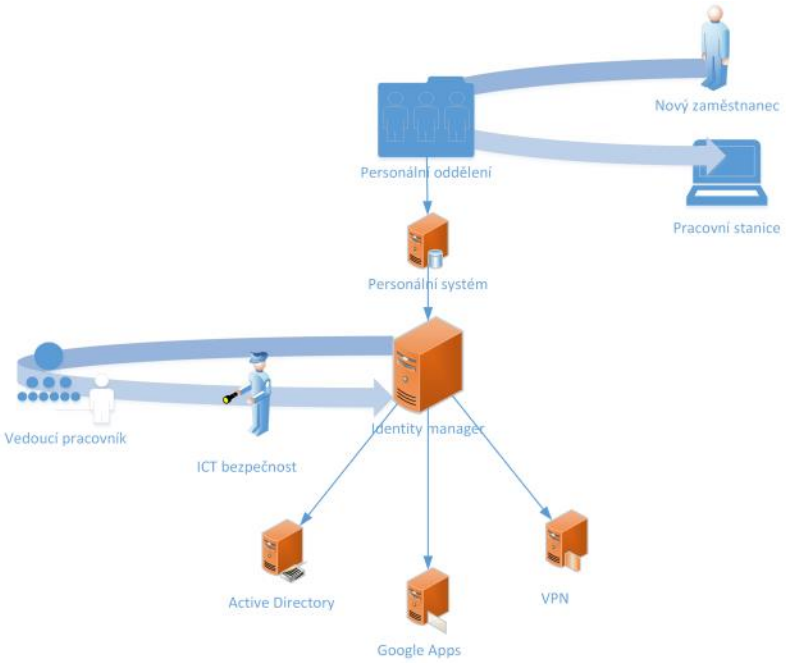
3.2.1.3 **Souhrn**

Výhody metodického přístupu jsou, že je rychlý na realizaci, dá se jednoduše aplikovat na firmy s různým stupněm organizovanosti práce.
„Nevýhody jsou: hodně lidských faktorů, náchylné k chybám, úmyslným i záměrným; může být časově náročné, v závislosti na vytížení správců systémů, nadřízeného a bezpečnosti; zaměstnanec vyřizuje agendu místo práce na pozici, na kterou byl přijat; proces jde po "hladké linii", spoléhá na dobrou vůli a loajálnost pracovníka; možnost vzniku nekonzistencí v informacích, vzhledem k různým cestám, jakými se informace aktualizují“ [4]
Metodický přístup je vhodný pro firmy s nízkým množstvím informačních systémů, kde je malý dopad zpronevěry informací a kde počet zaměstnanců málo fluktuuje.

3.2.2 **Technický přístup**

V technickém řešení je specializovaný systém Identity manager (Správce identit), který je zodpovědný za řízení identit a oprávnění. "Tento software obsahuje procesní a business logiku, potřebnou k tomu, aby byl uživatel automatizovaně zaveden do informačních systémů. Procesy a postupy zde slouží jako formální popis a pomůcka řízení identit a oprávnění.

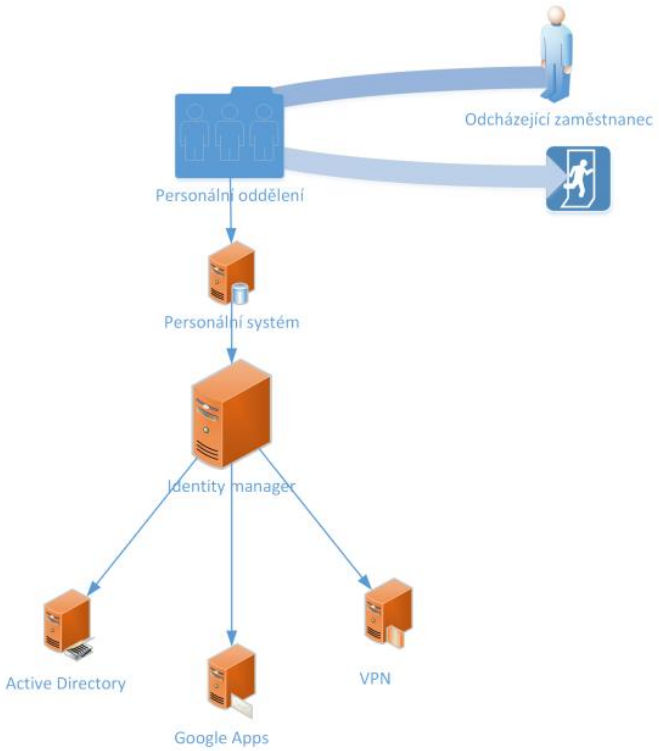
3.2.2.1 **Nástup nového zaměstnance**



Obrázek 4 - Nástup zaměstnance v technickém přístupu [4]

Nový zaměstnanec se dostaví na personální oddělení, kde jej zavedou do personálního systému. Vyplní odpovídající položky, jako jsou nacionále, oddělení, pracovní pozice, přímý nadřízený. Na základě těchto informací se v Identity manageru vyhodnotí sada pravidel: Má mít zaměstnanec e-mail? Kam má být zaveden do Active Directory? Má mít vzdálený přístup? Jakou roli má v rámci firemního intranetu? Výsledkem těchto pravidel je sada oprávnění, která je uživateli přiřazena. Pokud některé z nich vyžaduje schválení, je spuštěn schvalovací proces, ve kterém odpovědní pracovníci v prostředí Identity manageru provedou schválení. Následně Identity manager účty a oprávnění automaticky vytvoří a nastaví. Aktualizace informací je v tomto přístupu starostí Identity manageru. Ten si pravidelně kontroluje, zda se něco v některém systému nezměnilo. Má zaměstnanec nové telefonní číslo? Přešel pod jiný projekt? Vdala se pracovnice, takže je třeba ji přejmenovat? Na základě nastavených pravidel se provede automatická aktualizace informací v napojených informačních systémech, s případným spuštěním schvalování.

3.2.2.2 **Odchod zaměstnance**



Obrázek 5 - Odchod zaměstnance v technickém přístupu [4]

Odcházející zaměstnanec navštíví personální oddělení k vyřízení závěrečné agendy. Pracovníci oddělení změní stav zaměstnance v personálním systému – nastaví jej jako neaktivního, případně k nějakému budoucímu datu. Identity manager tuto informaci zpracuje, a pokud již nastal okamžik odchodu, definovaně ukončí uživatele v informačních systémech – odstraní, zneplatní, změní heslo, odebere oprávnění – dle nastavených pravidel“. [4]

3.2.2.3 **Souhrn**

Technický přístup má velké množství výhod: systém funguje autonomně, takže šetří správcům velké množství práce; existuje centralizovaný přehled o uživatelských účtech v systémech; riziko zneužití informací je minimální; změna oprávnění a informací je centralizovaná; umožňuje plánovat změny do budoucna; řešení umožňuje firmě dále rozvíjet ICT.

Mezi nevýhody lze zařadit vyšší technická složitost při vyšším počtu informačních systémů ve firmě, a také vyšší náklady na implementaci. Tento přístup je vhodný především pro střední a větší firmy, kde bezpečnost dat je důležitá, kde se používá více informačních systémů, nebo kde je velký počet uživatelů.

3.3 ITIL

Pro zajištění efektivity IT procesů ve firmě je vhodné dodržovat obecná doporučení podle ITIL. Information Technology Infrastructure Library (ITIL) je soubor nejlepších zkušeností mnoha společností z celého světa. Jedná se o mezinárodní standard pro řízení IT služeb, který umožňuje lépe využívat, plánovat a zkvalitňovat využití informačních technologií, a to z pohledu IT služeb, i z pohledu zákazníků. První verze ITIL byla vydána v letech 1989 až 1995 ve Velké Británii a skládala se z 31 knih. V letech 2000 až 2004 byla přepracována na ITIL v2, který byl složen ze 7 knih. V roce 2007 vyšel ITIL v3, který se skládá z 5 knih. V roce 2011 vyšla verze ITIL 2011 Edition, která vychází z verze v3, ale došlo v ní k sjednocení osnovy z všech 5 ústředních knih, a tím se celá struktura stala přehlednější. Verze ITIL 2011 Edition je aktuální do dnes.

ITIL je rozdělený do těchto částí: strategie služeb, návrh služeb, přechod služeb, provoz služeb, neustálé zlepšování služeb

3.3.1 Service Strategy

„Ústřední publikace poskytující praktický rámec k návrhu, vývoji a implementaci řízení služeb nejen z pohledu organizačního, ale i jako zdroje strategické výhody. Publikace obsahuje definice služeb, strategii ITSM a plánování přidané hodnoty, IT governance, definice typů poskytovatelů služeb a obchodních strategií, potažmo strategií služeb.

3.3.2 Service Design

Tato publikace poskytuje rámec pro návrh a vývoj služeb a procesů jejich řízení. Zahrnuje principy a metody pro převod strategických cílů do portfolia služeb. Nesoustředí se pouze na nové služby, ale obsahuje i procesy změny a průběžného zlepšování stávajících

služeb, potřebné pro udržení nebo zvýšení úrovně služeb, jejich přidané hodnoty pro zákazníka a v neposlední řadě i jejich soulad s právními normami a standardy.

3.3.3 Service Transition

Publikace obsahuje postup, jakým způsobem požadavky definované v rámci Service Strategy efektivně realizovat v průběhu Service Operation (reálné prostředí) za současného řízení rizik poruch a výpadků služeb. Poskytuje rámec pro řízení komplexní problematiky spojené se změnami ve službách a v procesech jejich řízení. Kombinuje postupy Release Managementu, Programme Managementu a Risk Managementu a převádí je do praktického kontextu řízení služeb jako celku.

3.3.4 Service Operation

Tato publikace obsahuje postupy pro řízení služeb v produkčním prostředí, dosažení výkonnosti a účinnosti v dodávce služeb a jejich podpoře tak, aby byla vyprodukována hodnota jak pro zákazníka, tak pro poskytovatele služby. Tato část ITIL® V3 v největším rozsahu přebírá knihy Service Strategy a Service Delivery ITIL® V2, ale také Application management a ICT infrastructure management.

3.3.5 Continual Service Improvement

Tato kniha obsahuje prostředky pro vytváření a udržování přidané hodnoty služby pro zákazníka prostřednictvím zvyšující se kvality služeb a efektivity jejich provozu. Kombinuje přitom principy, praktiky a metody řízení kvality a Change Managementu“. [5]

Obrázek 6 - Pokrytí jednotlivých oblastí v publikacích ITIL® V3 [5]

3.4 Hyper-V

Microsoft Hyper-V je virtualizační nástroj, který je dostupný na Windows 10 Enterprise, Pro a Education. Umožňuje na jednom fyzickém počítači s operačním systémem Windows spustit více virtuálních strojů s dalšími operačními systémy. Virtuální počítače nepřistupují k hardwarovým prostředkům fyzického počítače přímo, ale zprostředkovaně pomocí Virtual Machine Bus (VMBus). Každý virtuální stroj využívá svůj virtuální harddisk a má alokovanou určitou část operační paměti. Proto je nutné mít na fyzickém počítači dostatečné množství prostředků pro zajištění plynulého běhu.

S touto technologií je nyní mnohem snazší vytvořit testovací, školící nebo vývojová, a dokonce i produkční prostředí a přeměnit je v tvárné entity, které reagují na obchodní potřeby v okamžiku, kdy se objeví. Pro školící, vývojová a testovací prostředí je tato technologie obzvlášť užitečná, neboť je možné snadno znovu vrátit do svých původních nastavení vždy po dokončení určitého sezení. [6]

3.5 Windows Server

Windows Server 2016 je serverový operační systém vyvinutý firmou Microsoft jako součást rodiny operačních systémů Windows NT. Má společné jádro a další součásti s Windows 10. Protože se jedná o serverový operační systém, je určen pro nepřetržitý provoz aplikací a služeb.

„Prodávají se čtyři různé edice tohoto operačního systému: „Foundation“, „Essentials“, „Standard“ a „Datacenter“. Liší se především v licencích, maximálním počtu uživatelů a maximálním počtu procesorů v serveru. Edice „Foundation“ podporuje maximálně 15 uživatelů, 50 zařízení, 1 procesor, 32 GB RAM a licence se přiděluje jednomu fyzickému serveru. Edice „Essentials“ se oproti edici „Foundation“ liší tím, že podporuje 25 uživatelů, 2 procesory, 64 GB RAM a podporuje virtualizační funkci „Hyper-V“. Tyto dvě základní edice jsou vhodné pouze pro malé firmy o pár počítačích, pro větší firmy jsou vhodné edice „Standard“ nebo „Datacenter“. Edice jsou technicky shodné (maximálně 64 procesorů, 4 TB RAM a neomezený počet uživatelů a zařízení), ale „Datacenter“ umožňuje vytvořit neomezené množství virtuálních serverů. Pro testování bude použita edice „Standard“, protože obsahuje všechny potřebné funkce a licenčně je pro potřeby autora dostačující. Server s „Windows Server“ může mít role AD, DHCP, DNS a další“. [7]

3.5.1 GPO

Group Policy (skupinová politika) slouží k centrální správě počítačů, operačních systémů, aplikací a uživatelského nastavení v prostředí s Active Directory. Hlavní využití je tedy pro počítače zařazené do domény, kde umožňuje aplikovat jednotné nastavení na mnoho objektů zároveň. Existuje i verze Local Group Policy, která umožňuje v omezeném rozsahu řídit i samostatné, či nedoménové počítače.

Pomocí GPO lze instalovat jednoduché aplikace, nebo zvyšovat zabezpečení firmy omezením možností uživatele, například nastavení pravidla pro složitost uživatelova hesla, což zabraňuje uživateli zvolit příliš jednoduché heslo, zakázat přístup do Windows Task Manageru, aby uživatel nemohl vypnout sledovací nástroje či antivirový program, nebo zakázat přístup do některých složek, ve kterých by mohl uživatel omylem smazat systémové soubory.

3.5.2 **Windows PowerShell**

„Prostředí Windows PowerShell je prostředí příkazového řádku Windows, který je určený především pro správce systému. Prostředí Windows PowerShell obsahuje interaktivní řádku a skriptovací prostředí, které může být použito samostatně, nebo v kombinaci. Na rozdíl od většiny shell aplikací, které přijímají a vrací text, je prostředí Windows PowerShell postavené na rozhraní .NET Framework common language runtime (CLR) a .NET Framework, a přijímá a vrací .NET Framework objekty. Tato základní změna v prostředí přináší zcela nové nástroje a metody pro správu a konfiguraci systému Windows“. [8]

Skriptovací jazyk PowerShell je nejmladším skriptovacím jazykem v systému Windows, zastřešuje však doposud všechny známé skriptovací nástroje pro Windows, kde umožňuje manipulovat s různými objekty. Často podstatně zjednodušuje každodenní práci správců a uživatelů systému. Příkazy se běžně skládají ze dvou částí. První část tvoří sloveso, které značí, co se má udělat. Běžně jsou to slovesa: New, Get, Set, Remove, a další. Ve středu příkazu je pomlčka. Druhá část příkazu je tvořena předmětem (označení, nebo název objektu).

3.5.3 **SQL**

V praktické části jsou využívány některé nástroje, které pro ukládání dat využívají SQL databázi. „SQL (Structured Query Language) je zkratka pro standardizovaný strukturovaný dotazovací jazyk, který je používán pro práci s daty v relačních databázích. Umožňuje vytvářet databáze, plnit do nich informace a následně v nich vyhledávat podle zadaných kritérií. Má množinový přístup k datům a na databáze nahlíží jako na tabulky, což je pro uživatele snadné pochopit a s daty pracovat“. [7]

3.5.4 **IIS**

Pro nastavení webových portálů, ve kterých si uživatel může např. nastavit své bezpečností otázky, slouží IIS. „Internetová informační služba“ je softwarový webový server, který je součástí operačních systémů Windows, vytvoření společností Microsoft. Dle portálu W3Techs [9] se jedná o 3. nejpoužívanější webový server pro webové stránky.

3.6 Microsoft System Center

Všechny koncové stanice ve firmě Linet jsou instalovány pomocí nástroje „System Center“, který pomáhá zákazníkům získat možnosti jednotné správy datacentra díky přímo použitelným funkcím monitorování, nasazení, konfigurace, automatizace, ochrany a samoobsluhy.

„Skládá se ze šesti částí:

- Operations Manager (Monitoring)
- Data Protection Manager (zálohování)
- Orchestrator (Automatizace postupů)
- Service Manager (Helpdesk)
- Virtual Machine Manager (Virtualizace uživatelských počítačů)
- Configuration manager“ [7]

V prostředí, do kterého má být implementován Identity manager je používána pouze část Configuration manager.

3.6.1 Configuration Manager

„SCCM (System Center Configuration Manager), někdy nazýván také „ConfigMgr“, slouží pro komplexní řízení velkého počtu zařízení. Jedná se o nástroj pro správu zařízení nejen na platformě Windows. Umožňuje automatickou instalaci operačních systémů, aplikací a aktualizací. Uchovává v sobě databázi všech zařízení v síti, na kterých je nainstalována aplikace „SCCM Client“. Tato aplikace bývá zpravidla instalována automaticky. Dále též uchovává databázi všeho softwaru, který je na zařízeních nainstalován. Pro aplikační model platí zejména, že se provádí správa aplikací, nikoli skriptů“. [7]

3.7 Active Directory

„Active Directory je adresářová služba obsažená v systému Windows Server. Active Directory zahrnuje adresář, v němž jsou uloženy informace o vašich distribuovaných prostředcích, stejně jako o službách, díky nimž jsou tyto informace užitečné a dostupné.

Všechny verze systému Windows Server od systému Windows 20000 podporují Active Directory“ [10] V praxi se jedná o databázi počítačů, uživatelských účtů, jejich skupin práv a dalších entit, které je možné přehledně organizovat ve stromové struktuře.

3.7.1 Domény DNS

„Služba Active Directory používá službu DNS (Domain Name System). Služba DNS je standardní internetovou službou, která organizuje skupiny do hierarchické struktury. Třebaže jsou implementovány z různých důvodů, služby Active Directory a DNS mají stejnou hierarchickou strukturu. Hierarchie služby DNS je pro veřejné sítě definována na úrovni Internetu a pro privátní sítě na úrovni organizací. Různé úrovně v hierarchii služby DNS identifikují jednotlivé počítače a vztahy mezi počítači. Vztah mezi počítači je vyjádřen pomocí domén. Počítače, které jsou součástí stejné domény DNS, jsou blízce příbuzné. Domény použité v organizacích jsou organizačními doménami. Domény při kořeni hierarchie služby DNS jsou doménami nejvyšší úrovně, též kořenovými doménami“. [10]

3.7.2 Řadiče domény

„Při instalaci systému Windows Server na určitý počítač můžete tento počítač nakonfigurovat jako samostatný server, členský server nebo řadič domény. Řadič domény (též DC) je počítač, na kterém je uložen adresář služby Active Directory“. [10]

3.7.3 Objekty služby Active Directory

„Prostředky, které chcete reprezentovat ve službě Active Directory, jsou vytvořeny a uloženy jako objekty. Objekty mají atributy, které definují druh informací, jež chcete o těchto prostředcích uložit. Například objekt Uživatel (User) v Active Directory obsahuje atributy, které pomáhají popsat uživatele, tedy např. jméno, iniciálu druhého jména, příjmení a zobrazované jméno. Objekt Počítač (Computer) v Active Directory obsahuje atributy, které pomáhají popsat počítače, tedy např. název počítače, popis, umístění a identifikátor zabezpečení“. [10]

3.7.4 Domény

Domény jsou logickými seskupeními objektů, které sdílí společné databáze služby Active Directory. V adresáři jsou domény reprezentovány jako objekty kontejneru. V doméně je možné vytvářet účty pro uživatele, skupiny a počítače, stejně jako pro sdílené prostředky, jako jsou tiskárny a složky.

3.8 Azure AD

Azure Active Directory je cloudová adresářová služba. „Pomáhá spravovat identity uživatelů a vytvářet zásady přístupu s využitím inteligentních funkcí pro zabezpečení vašich prostředků. Služba Azure AD, která je základní komponentou Office 365, Azure a Enterprise Mobility + Security, centralizuje správu identit a přístupu a zajišťuje kvalitní zabezpečení, produktivitu a správu napříč zařízeními, daty, aplikacemi i infrastrukturou“. Slouží pro autentizaci v cloudových službách (Office 365, Exchange Online, Share Point Online, Skype for Business, Azure App Service a další). „Služba Azure AD je navržená tak, aby fungovala pro aplikace v cloudu, na mobilní platformě i v místním prostředí a umožňovala vrstvit funkce zabezpečení, jako je třeba podmíněný přístup, pro zvýšení ochrany uživatelů a vaší firmy“. Na rozdíl od on-premise Active Directory neumožňuje nastavování práv na složky. Synchronizace z on-premise AD do Azure AD probíhá pouze jednostranně.

„Díky použití jedné identity uživatelé mohou spouštět všechny svoje cloudové aplikace z individuálního webového přístupového panelu nebo mobilní aplikace a používat stejné prostředí bez ohledu na to, jestli pracují se zařízeními se systémem Windows, Mac, Android nebo iOS. Proxy aplikací služby AD vám umožní dostat se nad rámec cloudových aplikací, publikovat místní webové aplikace a zajistit vysoce zabezpečený vzdálený přístup a jednotné přihlašování“. [11]

3.8.1 Azure AD Privileged Identity Management

Globální administrátor může v Azure AD přiřadit uživatelům v organizace různé administrátorské role. Tyto role umožňují určit, jaké úkoly, jako například přidání a odebrání

uživatele, či změnu nastavení služby, může uživatel provést v Azure AD, Office 365 a dalších službách Microsoft Online.

Hlavní, globální administrátor může určit, zda je administrátorská role přiřazena na trvalo, nebo pouze na dočasnou dobu. „Azure AD Privileged Identity Management (PIM) spravuje zásady pro privilegovaný přístup pro uživatele ve službě Azure AD. PIM uživatelům přiřadí jednu nebo více rolí ve službě Azure AD a globální administrátor může rozhodnout, zda role bude na trvalo, nebo pouze dočasně. Když má uživatel trvale přiřazenou roli, nebo se aktivuje dočasně přiřazená role, pak může spravovat služby Azure Active Directory, Office 365 a dalších aplikací.

V oprávnění trvalého a dočasného administrátorského přístupu není žádný rozdíl. Jediným rozdílem je, že někteří uživatelé nepotřebují tento přístup neustále. Role administrátora je přiřazována pouze, když ji potřebují, čím je výrazně zvýšena bezpečnost“.

PIM umožňuje přiřadit uživatelům běžné role správce, včetně:

- **Globální správce** – správce společnosti, má přístup ke všem administrativním funkcím. Organizace může mít i více než jednoho globálního správce. Osoba, která se zaregistruje při nákupu předplatného Office 365 se automaticky stává globálním správcem.
- **Správce privilegovaných rolí** – spravuje Azure AD PIM a aktualizuje přiřazení rolí pro ostatní uživatele.
- **Správce fakturace** – má oprávnění dělat nákupy, spravovat předplatné, spravovat servisní požadavky a sledovat stav služeb
- **Správce hesel** – může resetovat hesla, spravovat žádosti o služby a sledovat stav služeb. Správci hesel jsou omezeni na resetování uživatelských hesel.
- **Správce služeb** – spravuje žádosti o služby a sleduje stav služeb.
- **Správce uživatelů** – má možnost resetovat hesla, sledovat stav služeb, spravovat uživatelské účty, skupiny uživatelů a žádosti o služby. Správci uživatelů nelze odstranit globálního správce, vytvářet další role správců, ani resetovat hesla správců fakturace, služeb a globálních správců.
- **Správce Exchange** – má přístup na Exchange Online pro správu prostřednictvím Exchange Admin Center (EAC).

- **Správce služeb Sharepoint** – má přístupová oprávnění k Sharepoint Online prostřednictvím Sharepoint Admin Center.
- **Správce Skype pro firmy** – má administrátorský přístup ke Skype pro firmy prostřednictvím Skype pro firmy Admin Center“. [12]

3.9 Srovnání produktů pro Identity Management

Firma dosud využívá produkty od společností Microsoft, Oracle a Salesforce, proto byly porovnány nabízené řešení těchto firem.

3.9.1 Microsoft Identity Manager

„Microsoft Identity Manager 2016 vytváří vazby mezi řešeními pro správu identit a přístupu od společnosti Microsoft transparentním přemostěním několika místních úložišť pro ověřování, například Active Directory, LDAP, Oracle, a dalších aplikací s adresářem Azure Active Directory. Tato funkce poskytuje konzistentní možnosti a prostředí pro místní obchodní aplikace i pro řešení SaaS“. [13]

Microsoft vstoupil na trh IDaaS v roce 2014 vydáním služby Azure Active Directory Premium. Od té doby tento technologický gigant značně ovlivnit trh. AAD nabízí srovnatelné funkce s dalšími nabídkami IDaaS a zahrnuje přístup k produktům Microsoft Identity Managet pro použití s On-premise systémy. Nabízí také služby Active Directory, federační služby a cloudové služby pro více uživatelů, které jsou svázány s EMM (Enterprise Mobility Management) a se správou oprávnění, a jsou podporovány 28 datacentry po celém světě.

3.9.1.1 Klíčové vlastnosti

- **Private Cloud Architecture** – Služba Azure Active Directory poskytuje zabezpečené jednotné přihlášení do lokálních i cloudových aplikací, včetně aplikací Microsoft Office 365 a tisíců dalších SaaS aplikací, jako jsou Salesforce, Workday, DocuSign, ServiceNow a Box.
- **Fast Onboarding** – řízení přístupů na základě faktorů, jako je lokace, citlivost aplikací a stavu zařízení.

- **Advanced Monitoring** – cloud-based, robustní analýza a strojové učení poskytující smysluplné informace a automatizované zásady založené na rizicích, které mohou pomoci chránit identitu před budoucími hrozbami.

3.9.1.2 Souhrn

Společnost Microsoft poskytuje silný nástroj pro podniky, které již využívají produkty z portfolia Microsoftu, nebo kdo již používá cloudovou službu Microsoft Azure a hledají základní funkce pro správu identity. Zákazníci hledající řešení pro oblast B2C by ale měli být obezřetní, protože Microsoft ještě má co dohánět oproti konkurenci. Možnosti více faktorového ověřování a self-service obnovy hesla jsou na dobré úrovni. Průměrná cena licencí je o něco vyšší, než u konkurence.

3.9.2 Oracle Identity Governance

„OIG (Oracle Identity Governance) je integrovaný systém, který centralizuje bezpečnost pro aplikace a webové služby, a poskytuje jednotný kontakt pro podporu. OIG je vhodný a doporučovaný pro velké firmy. Přestože je velmi komplexní a flexibilní, mohl by být příliš přehnaný pro malé a středně velké podniky. Or roku 2016 Oracle navíc nabízí službu Oracle identity Cloud Service (IDCS). Oracle je významným hráčem v oblasti IT v podnicích a řešení OIG je velmi doporučováno do prostředí, které již využívá některé z produktů Oracle.

3.9.2.1 Klíčové vlastnosti

- **Self-Service Access** – přizpůsobitelný rámec uživatelského rozhraní, který je trvanlivý během inovací a oprav.
- **Identity Inteligence** – inteligentní a flexibilní zjišťování rolí pro efektivní správu a dodržování zásad.
- **Privileged Account Management** – výsadní řízení účtů pro řízení přístupu ze sdílených účtů, a poskytuje bohaté informace pro audit, aby byla zajištěna vysoká bezpečnost a shodu v citlivých systémech.

- **Identity Auditor** – pokročilá integrovaná analytika pro certifikaci přístupu, která je součástí zajišťovacího procesu pro přesnost a efektivitu.

3.9.2.2 Souhrn

Modulární řešení správy identit společnosti Oracle je vhodné pro velké organizace s komplexními potřebami IGA (Identity Governance and Administration), ale nejvíce je doporučováno pro ty, kteří již provozují portfolio produktů Oracle. Zdá se však, že je předurčeno budoucím inovacím: může podporovat širokou škálu webových aplikací a cloud architektury, má na trhu velké zastoupení a dokáže zvládnout nároky velkých firem“. [14]

3.9.3 Salesforce

Obrázek 7 - Logo Salesforce [15]

Salesforce je především platforma pro řízení vztahů se zákazníky, se zaměřením na prodej, service a marketing. V roce 2013 vstoupili na trh Identity managementu s vydáním Salesforce Identity, řešení IDaaS, které je nabízeno jako nezávislá služba, i jako součást nabídky Salesforce Cloud PaaS (Platform-as-a-Service). Nabízí základní možnosti IDaaS pro správu přístupů a služeb, stejně jako vynikající grafické workflow pro správu politik, podnikových sociálních identit a centralizované správy přístupů.

3.9.3.1 Klíčové vlastnosti

- **Cloud-based User Directories** – uživatelské účty a informace jsou uloženy a uchovávány na jednom místě, zatímco jsou dostupné ostatním službám a aplikacím.
- **Authenticitaion Services** – ověřuje uživatele a udržuje kontrolu nad jejich uživatelským přístupem.

- **Access Management** – poskytuje správu přístupu a oprávnění pro aplikace třetích stran, včetně integrace uživatelského rozhraní, takže aplikace a služby uživatelů jsou k dispozici ke kontrole.
- **App User Provisioning** – zjednodušuje proces poskytování a odebírání přístupu k aplikacím více uživatelům současně.
- **Salesforce Identity Connect** – Integruje službu Microsoft AD se službou Salesforce a umožňuje současně správu uživatelů AD a Salesforce.

3.9.3.2 Souhrn

Řešení společnosti Salesforce IDaaS je k dispozici jako nezávislá služba, ale je nejvhodnější pro organizace, které působí v oblasti služeb zákazníkům a maloobchodu, kde společnost Salesforce má nejvýznamnější podíl na trhu. Salesforce se stále přizpůsobuje trhu Identity Managementu a podpoře jejich nezávislých služeb, takže zatím nemusí být tolik vyspělý, jako vyžadují větší podniky, které se neorientují na zákazníky (B2C). [14]

3.9.4 Souhrn

Řešení od firmy Oracle je vhodné především pro webové aplikace Oracle, které jsou ve firmě používány velmi zřídka. Produkt od Salesforce je určen především pro B2C (Business to Customer) sektor. Microsoft Identity Manager se tak jeví jako jediné vhodné B2B (Business to Business) řešení pro firmu založenou především na prostředí Microsoft. Na rok 2019 je již naplánovaný přechod z MS Office on-premise na MS Office 365 a s tím související napojení Active Directory na MS Azure Active Directory. Také z těchto důvodů bylo vybráno řešení od společnosti Microsoft, které pouze rozšíří možnosti již používaných produktů.

4 Vlastní práce

Vlastní práce se skládá z představení firmy Linet, z analýzy současného stavu pro odhalení problémů, které budou v této práci řešeny. Dále z přípravy testovacího prostředí, které vychází ze skutečného prostředí firmy, propojení testovacího AD do Azure AD a testování samoobslužného resetu hesla. Následuje implementace MIM a nastavení synchronizace s AD, testování samoobslužného resetu hesla, a návrh napojení AD na HR databázi zaměstnanců. Poté je provedena finanční analýza.

4.1 Představení firmy

Obrázek 8 - Logo firmy linet [16]

Předmětem práce je zlepšení služeb pro koncové uživatele ve firmě Linet. „LINET spol. s r.o. je součástí skupiny LINET Group SE, předního světového výrobce zdravotnických lůžek. Svého postavení firma dosáhla zejména díky inovacím, které zkvalitňují úroveň zdravotní péče ve více než sto zemích.“ [16] Prodeji a servisu lůžek pomáhá 15 dceřiných společností, které jsou rozmístěné po celém světě. IT podpora, která je centralizovaná v České republice ve Slaném, je rozdělena na 3 úrovně. První úroveň má 7 členů a autor je lídrem tohoto týmu. Na druhé úrovni je 5 členů a na třetí pouze 1. V celé firmě je 1 společná doména, veškerý hardware je značky Dell a všechny koncové stanice využívají operační systém Windows, který je instalován pomocí SCCM [Kapitola 3.6].

4.2 Analýza současných problémů

Analýza vychází ze statistického sledování servisních požadavků a z kontroly nastavení bezpečnostní politiky

4.2.1 Uživatelská hesla s neomezenou platností

Při kontrole nastavení uživatelských účtů v AD bylo zjištěno velké bezpečnostní riziko způsobené tím, že všechny účty mají hesla s neomezenou platností a s nízkou složitostí. Před nastavením platnosti pouze na dobu 2 měsíců je ale nutné uživatelům umožnit si heslo samoobslužně resetovat, aby nedošlo k navýšení vytížení IT podpory a aby nemusela být resetovaná hesla přenášena uživateli v nezašifrované podobě.

4.2.2 Příliš dlouhá tvorba nového uživatelského účtu

Tvorba uživatelského účtu od založení požadavku do předání přihlašovacích údajů novému zaměstnanci trvá průměrně 4 dny, během kterých nový zaměstnanec nemůže pracovat. Schvalovací proces trvá průměrně 1 den, až poté je požadavek připraven k řešení podporou IT, kde požadavek čeká ve frontě dříve zadaných požadavků. Proto je třeba najít systém, který účet po schválení automaticky vytvoří podle údajů definovaných personálním oddělením, čímž dojde ke snížení počtu servisních požadavků a zrychlení procesu tvorby nového účtu.

4.2.3 IT podpora není informována o změnách

Při změně pozice zaměstnanec IT požádá o nová práva, která jeho nová pozice vyžaduje, což mu jeho nadřízený schválí. IT podpora ale nedostane informaci o odebrání práv, která již zaměstnanec na nové pozici nepotřebuje. Uživateli tyto práva zůstávají a ve firmě není nastaven proces, který by nepotřebná práva odebral. Uživatelům jsou přidělována jednotlivá práva, ne definované role dle pozice.

Pokud odcházející zaměstnanec sám neinformuje IT oddělení o svém odchodu, je o tom IT informováno až na konci měsíce. V případě, že k takovému odchodu dojde v průběhu měsíce, vzniká riziko zneužití aktivního účtu.

4.3 Navrhované řešení

Navrhované řešení zjištěných problémů má 2 fáze:

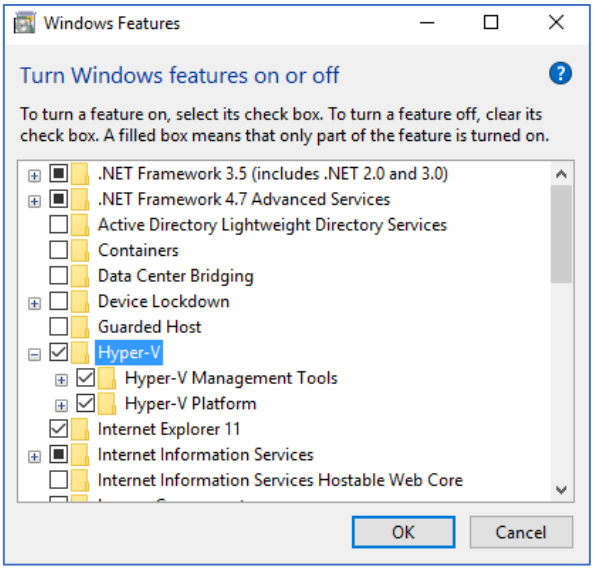
- Nastavení samoobslužného resetu hesla

- Propojení AD s HR databází

Samoobslužný reset hesla je možné nastavit v Azure AD, i v MIM. V této práci budou otestovány obě možnosti a porovnány. K propojení AD s HR databází bude využit nástroj MIM. Před implementací navrhovaných řešení je potřeba připravit testovací prostředí.

4.4 Příprava testovacího prostředí

Fyzický testovací stroj využívá Windows 10 Pro verze 1803. Pro testování bylo zvoleno virtuální prostředí Hyper-V [Kapitola 2.4], které je v této verzi operačního systému zabudované a autor s ním již má zkušenosti. Virtuální prostředí bylo nutné nejprve povolit v nabídce „Turn Windows features on or off“.



Obrázek 9 - Povolení virtuálního prostředí Hyper-V [Vlastní tvorba]

Po povolení byl fyzický testovací stroj restartován a poté se v počítači zobrazila aplikace „Hyper-V Manager“, která slouží pro tvorbu virtuálního testovacího prostředí.

4.4.1 Tvorba virtuálního switche

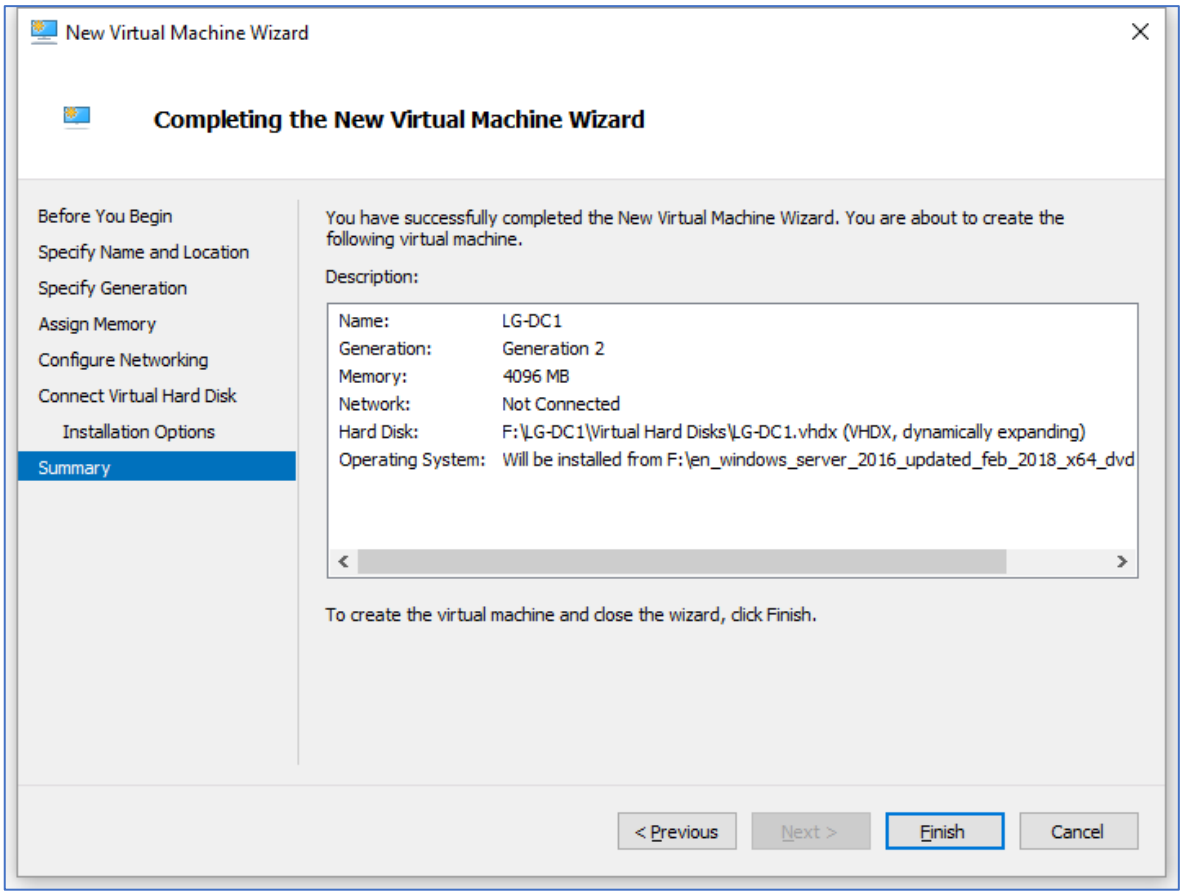
Aby mohly virtuální stroje přistupovat k internetu, či k vnitřní síti, je potřeba v Hyper-V vytvořit virtuální switch. Na výběr je ze tří druhů: externí, interní a privátní. První z nich se napojuje na fyzický síťový adaptér a virtuální stroje tak mohou přistupovat k fyzické síti, potažmo k internetu. Druhý, interní, slouží pro propojení virtuálních strojů

a fyzického počítače, na kterém je virtuální prostředí vytvářeno, neumožňuje připojení k internetu. Třetí, privátní switch, propojuje pouze virtuální stanice, bez přístupu k fyzickému počítači.

Pro instalaci nejnovějších aktualizací na všechny stroje bude potřeba připojení k internetu, autor tedy vytvořil jeden externí virtuální switch: „External_switch“, pokud ale připojení k internetu nebude potřeba, je vhodné stroje přepojit na privátní switch, čím dojde k zajištění vyšší bezpečnosti. Proto auto vytvořil druhý privátní: „Private_switch“.

4.4.2 Tvorba serveru LG-DC1

V okně „Hyper-V Manager“ byl vytvořen virtuální stroj LG-DC1 s umístěním na prázdném SSD disku o velikosti 180 GB, který byl vyčleněn pro účely testovacího prostředí. „V prvním kroku bylo na výběr, zda vytvořit virtuální stroj s výchozími hodnotami, nebo s přizpůsobenou konfigurací. Byla zvolena přizpůsobená konfigurace, aby bylo možné vše nastavit podle potřeb. V dalším kroku bylo na výběr, zda má být použit virtuální stroj generace 1 nebo 2. Generace 1 podporuje i 32 bitové operační systémy a také virtuální hardware, dostupný ve starších verzích „Hyper-V“. Generace 2 podporuje pouze 64 bitové operační systémy, nabízí „UEFI firmware“ a nejnovější virtualizační funkce. Vzhledem k vyšší rychlosti pod „UEFI firmwarem“ a nižší hardwarové náročnosti byla zvolena generaci 2. V dalším kroku byla volena velikost operační paměti virtuálního stroje. Pro nastavování bylo zvoleno 4096 MB z dostupných 16 GB. Bylo povoleno použití dynamické paměti pro tento virtuální stroj, „Hyper-V“ díky tomu bude moci automaticky měnit sdílené zdroje (paměť) pro vyšší výkon. Zároveň bude možné manuálně měnit velikost využité paměti i za běhu virtuálního stroje“. [7]



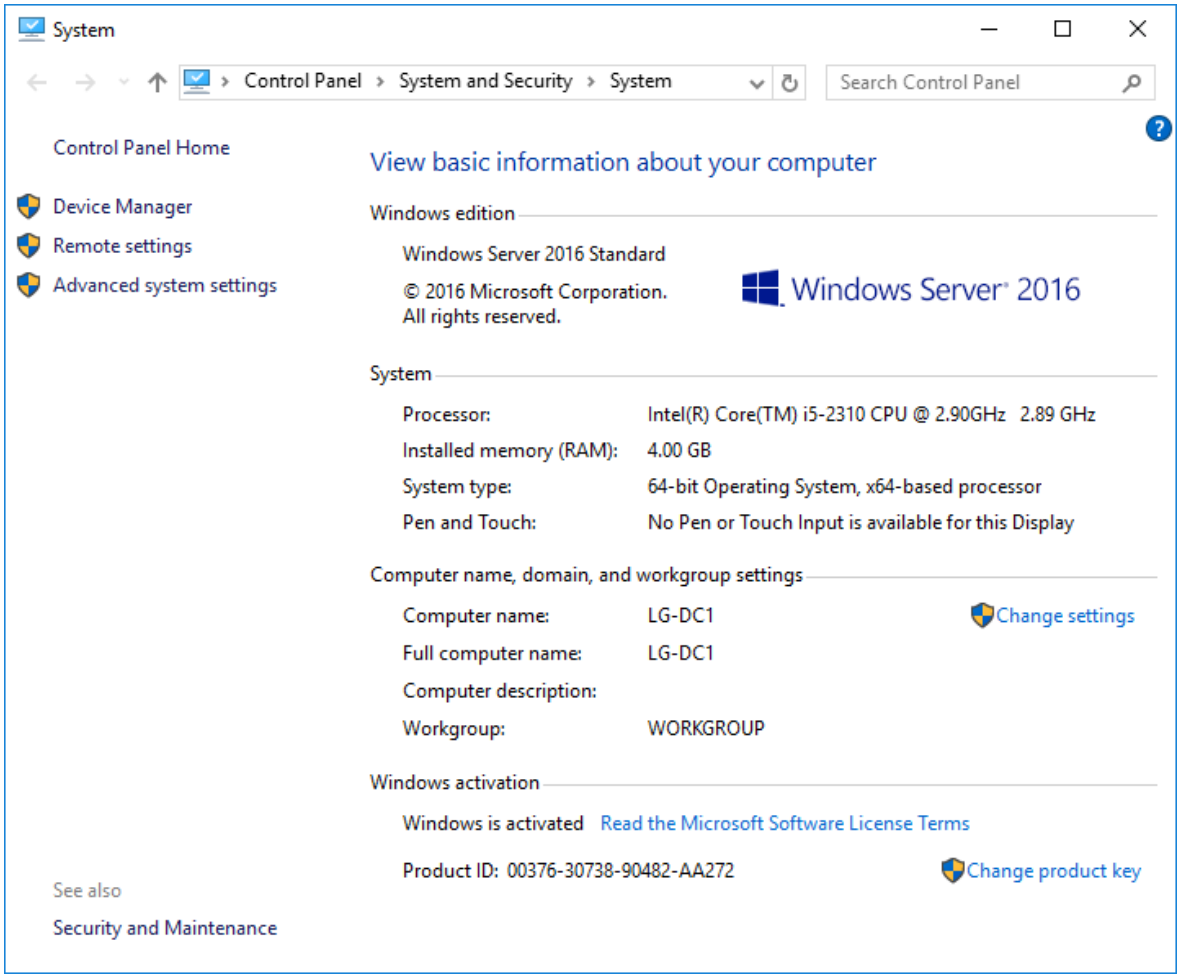
Obrázek 10 - Souhrn nastavení virtuálního stroje LG-DC1 [Vlastní tvorba]

4.4.2.1 Instalace operačního systému

Firma LINET používá na všech doménových řadičích „Windows Server 2013 Standard“, ale vzhledem k plánovanému povýšení na verzi „Windows Server 2016 Standard“ se autor rozhodl použít novější verzi z roku 2016. Instalační médium bylo staženo zdarma pro studijní účely ze stránek DreamSpark [17]. Bylo připojeno jako virtuální DVD mechanika pomocí SCSI kontroleru a z něj byla spuštěna instalace. Aby šla instalace úspěšně spustit, musel být instalační soubor fyzicky uložený na jiném disku, než na kterém je virtuální stroj. Při instalaci bylo na výběr ze dvou verzí: s grafickým rozhraním a bez. Pro efektivní správu zvolil autor verzi „Desktop Experience“ s grafickým rozhraním. Po dokončení instalace byl stroj připojen k internetu prostřednictvím externího switche a nainstalovány všechny nejnovější aktualizace.

4.4.2.2 **Základní nastavení serveru**

Stroj byl přejmenován z „WIN-82KF8KOJENO“ na „LG-DC1“, ale zatím byl ponechán v pracovní skupině „WORKGROUP“. Byl vytvořen záložní uživatelský účet OEM bez hesla a ten byl přidán do lokální skupiny „Administrators“. Byla nastavena statická IP adresa pro privátní síť 10.0.1.1, maska podsítě 255.255.255.0, výchozí brána 10.0.1.1 a preferovaný DNS server 10.0.1.1, protože v dalším kroku bude stroj LG-DC1 povýšen na doménový řadič, DHCP a DNS server.

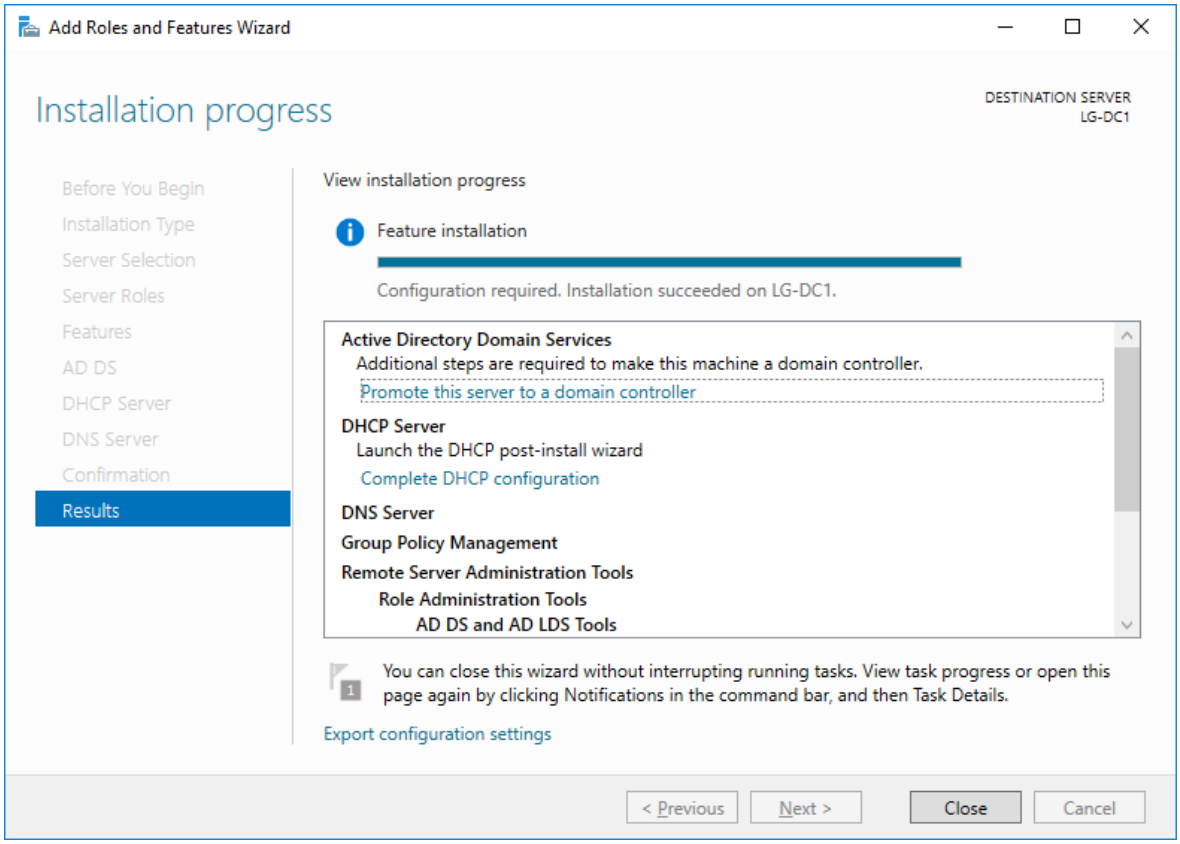


Obrázek 11 – Přehled informací o LG-DC1 [Vlastní tvorba]

4.4.3 **Povýšení serveru LG-DC1 na doménový řadič**

V okně „Server Manager“ bylo zvoleno „Add Roles and Features Wizard“. V prvním kroku byl autor upozorněn, že je potřeba ověřit, že má účet „Administrator“ dostatečně bezpečné heslo, že má server nastavenou statickou IP adresu a že byly nainstalovány

nejnovější bezpečností aktualizace. Server všechny body splňuje. V druhém kroku bylo třeba vybrat mezi verzí „Role-based or feature-based installation“ a „Remote Desktop Services installation“. První slouží pro nastavení jednoho serveru s rolemi a službami, druhá pro tvorbu infrastruktury pro virtuální klientské stanice. Pro účely doménového řadiče byla zvolena první možnost. Poté byl zvolen server LG-DC1, který má být povýšen. Ve čtvrtém kroku byly zvoleny všechny role, které má tento server mít: „Active Directory Domain Services“, „DHCP Server“ a „DNS Server“. Poté byl autor upozorněn, že pro zajištění dostupnosti je nutné mít minimálně 2 doménové řadiče pro každou doménu. Druhý bude vytvořen a přidán později. Před spuštěním instalačního procesu bylo zvoleno, aby se server v případě potřeby automaticky restartoval. Role, které byly přidány bez jediného restartu, bylo následně nutné korektně nastavit.

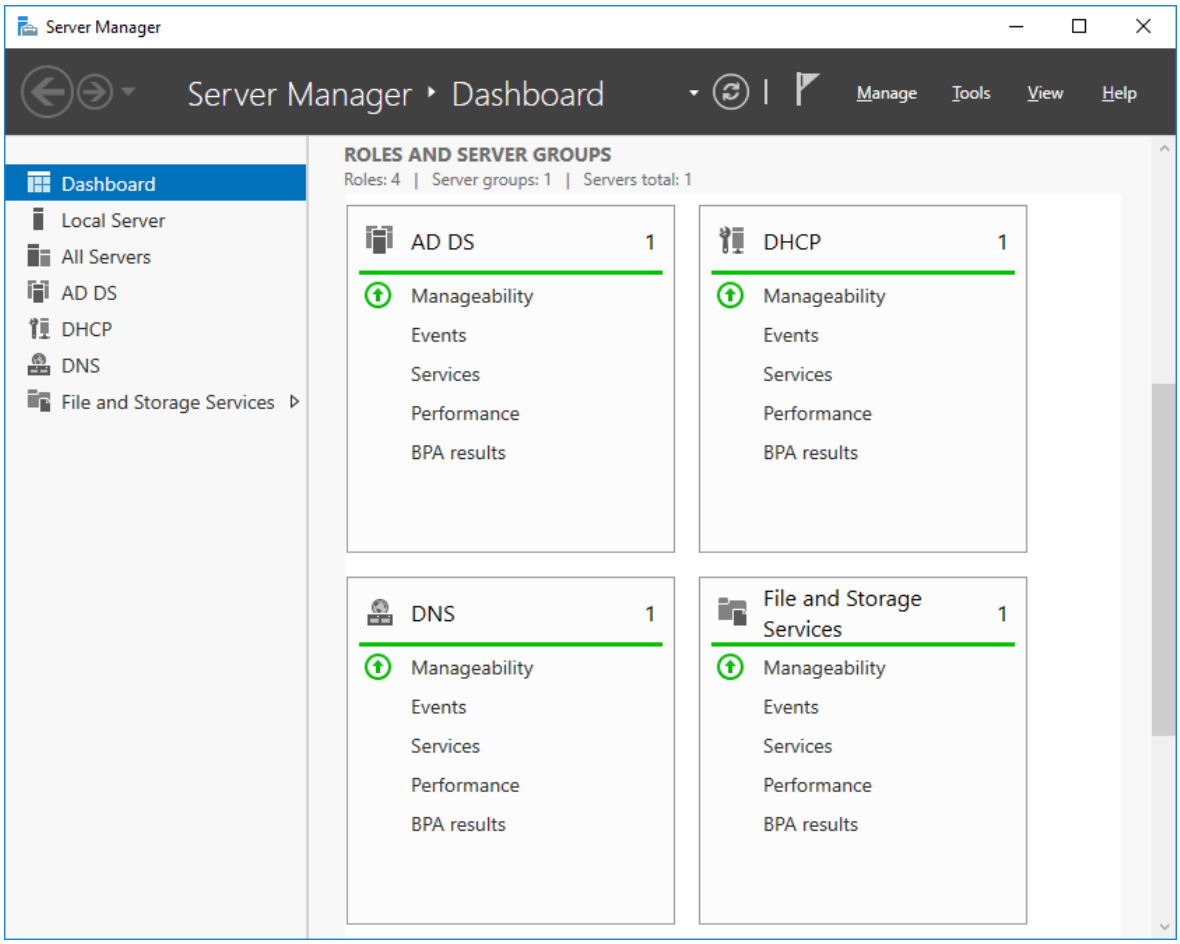


Obrázek 12 - Přidání rolí DC, DHCP a DNS [Vlastní tvorba]

4.4.3.1 Nastavení doménového řadiče

Po zvolení dokončení povýšení serveru na doménový řadič měl autor na výběr mezi třemi možnostmi: přidat doménový řadit k již existující doméně, přidat novou doménu do

již existujícího lesa, nebo vytvořit nový les. V testovacím prostředí ještě neexistovala žádná doména, ani les, proto byla zvolena třetí možnost. Doména byla pojmenována „LINET-GROUP.LOCAL“ podle reálného prostředí firmy Linet. Poté bylo třeba zvolit funkční úroveň lesa, který se určuje podle nejstarší verze operačního systému, který v lese je. V tomto testovacím prostředí autor použil pouze Windows Server 2016 či 2019, proto ponechal možnost Windows Server 2016. Dále bylo zadáno heslo pro obnovení „Directory Services Restore Mode“ (DSRM). V následujícím kroku byla možnost změnit „NetBIOS domain name“, ale bylo ponecháno „LINET-GROUP“. Cesta pro uložení systémových souborů byla ponechána výchozí „C:\Windows\“. Po spuštění instalace byl vyžadován restart pro dokončení procesu. Po restartu již byl doménový řadič připraven.



Obrázek 13 - Přehled rolí serveru LG-DC1 [Vlastní tvorba]

4.4.3.2 Nastavení DHCP

Přidělování IP adres zařízením v síti pomocí DHCP bylo nastaveno v panelu: „Administrative Tools - DHCP – LG-DC1.linet-group.local – IPv4 – right-click – New Scope“. Jméno i popis byly zvoleny „VLAN1“, počáteční IP adresa: 10.0.1.11 a konečná: 10.0.1.192, maska podsítě: 255.255.255.0. Doba trvání jedné přidělené adresy byla ponechána na výchozích 8 dní. Výchozí brána byla nastavena na IP adresu hlavního řadiče: 10.0.1.1. Po potvrzení bylo DHCP nakonfigurované.

Poté bylo potřeba DHCP autorizovat, aby mohlo přiřazovat IP adresy. Jedná se o bezpečnostní opatření, aby v doméně přiřazovaly IP adresy pouze ověřené servery. Pro autorizaci bylo v nastavení DHCP kliknuto na název server „lg-dc1.linet-group.local“ a zvoleno „Authorize“, po chvíli se u IPv4 a IPv6 objevilo zelené kolo, značící, že je DHCP funkční.

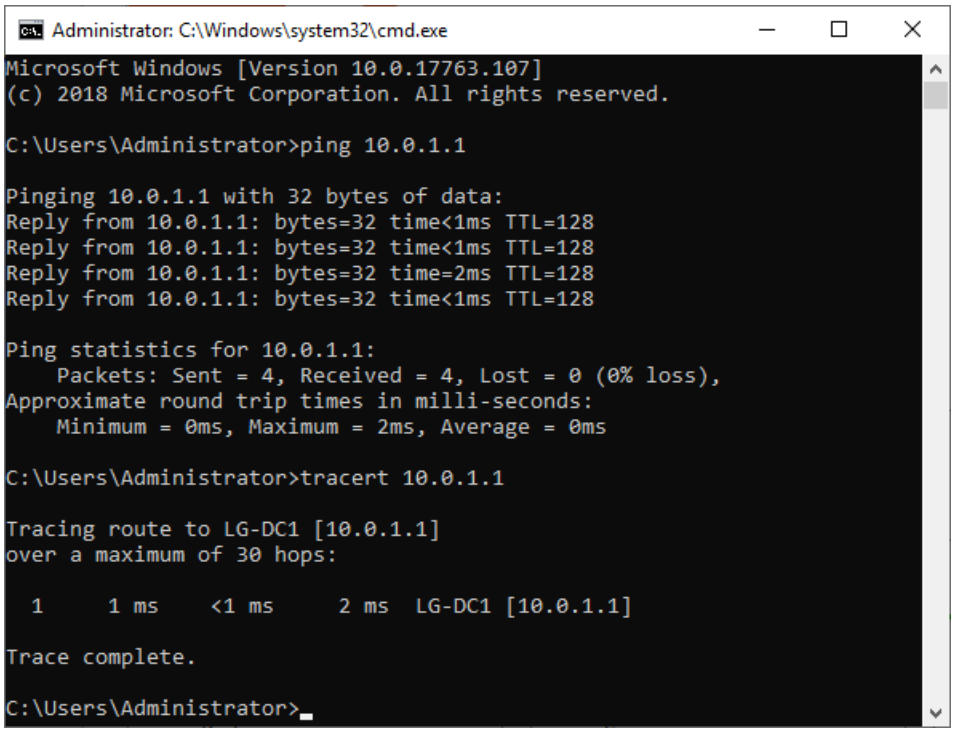
4.4.3.3 Vytvoření kontrolního bodu

Hyper-V umožňuje vytvořit kontrolní bod, ke kterému je možné se v případě jakýchkoliv problémů vrátit. Je proto doporučováno po každé větší změně tyto kontrolní body vytvářet. V seznamu virtuálních stanic v Hyper-V bylo kliknuto pravým tlačítkem na stanici LG-DC1 a zvoleno „Checkpoint“. V dolním okně „Checkpoints“ se zobrazil nový kontrolní bod s datem a časem, kdy byl vytvořen. Pro lepší orientaci byl za současný název doplněn popis: „Domain and DHCP set“.

4.4.4 Příprava záložního serveru LG-DC2

Pro zajištění vyšší dostupnosti řadičů je třeba mít alespoň 2 doménové řadiče, které se vzájemně replikují. Proto byl vytvořen nový server s názvem „LG-DC2“ se stejným nastavením, jako má server LG-DC1. Na tento server se autor rozhodl nainstalovat nejnovější verzi „Windows Server 2019 Standard“ pro otestování rozdílů oproti verzi 2016. Instalační klíč byl získán na webových stránkách Microsoft Dreamspark [17]. Verze byla zvolena s grafickým rozhraním. Po instalaci bylo zvoleno stejné heslo, jako v případě prvního serveru.

Server byl přejmenován z automaticky generovaného názvu „WIN-PL4G82U9CM9“ na „LG-DC2“. Dále mu byla přiřazena statická IP adresa 10.0.1.2, maska 255.255.255.0, výchozí brána, i preferovaný DNS server jsou shodné s IP adresou serveru LG-DC1, tedy 10.0.1.1. V příkazovém řádku bylo pomocí příkazů „ping“ a „tracert“ na IP adresu serveru LG-DC1 ověřeno, že jsou servery ve stejné síti.



Obrázek 14 - Ověření komunikace mezi servery [Vlastní tvorba]

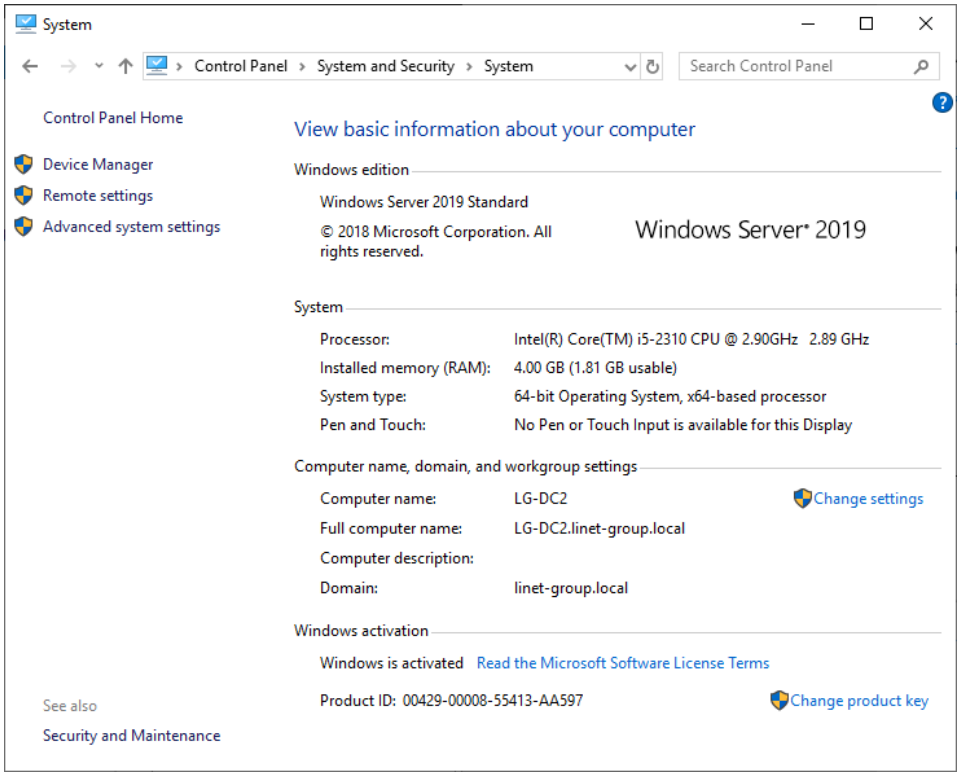
K virtuální stanici byl připojen druhý virtuální síťový adaptér a ten nastaven na „External_switch“ pro stažení nejnovějších aktualizací a aktivaci Windows. Po jejich stažení bylo potřeba server restartován a síťový adaptér „External_switch“ byl opět odebrán pro zajištění bezpečnosti.

4.4.4.1 **Připojení serveru LG-DC2 do domény**

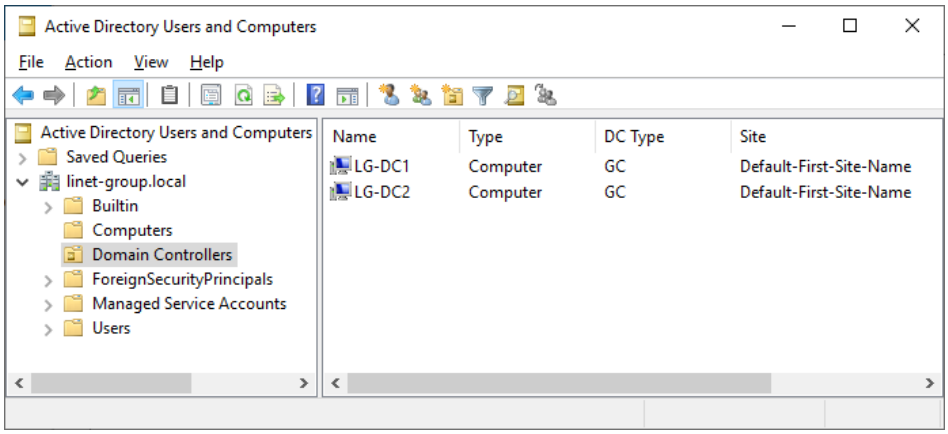
První část připojování nového doménového řadiče do již existující domény do role záložního doménového řadiče byla shodná s postupem pro tvorbu nového doménového řadiče. V okně „Server Manager“ bylo kliknuto na „Add roles and features“, první tři kroky byly, stejně jako v prvním případě, beze změny potvrzeny. Ve čtvrtém kroku byla zvolena pouze role „Active Directory Domain Sevices“. Pátý krok byl beze změny potvrzen,

v šestém byla zaškrtnuta volba pro automatický restart v případě potřeby. Pro nainstalování ale restart opět nebyl potřeba.

Následující postup se již liší. V druhé části povyšování serveru na doménový řadič bylo v okně „Deployment Configuration“ zvoleno přidat doménový řadič do již existující domény. Pro volbu domény „linet-group.local“ bylo nutné vyplnit kredence doménového administrátorského účtu „linet-group\administrator“. V dalším kroku měl autor možnost volby, zda má být doménový řadič pouze pro čtení. Tato možnost je vhodná pro zrychlení ověřování například ve vzdálené pobočce firmy, při zachování vysoké bezpečnosti. V tomto případě ale zvolena nebyla. Všechny další kroky byly beze změny potvrzeny, v posledním bylo zkontrolováno, že server splňuje všechny vyžadované prerekvizity a poté spuštěna instalace. V jejím průběhu byl vyžadován restart, po kterém byl již server součástí domény „linet-group.local“.



Obrázek 15 - Server LG-DC2 součástí domény [Vlastní tvorba]



Obrázek 16 - Přehled doménových řadičů v AD [Vlastní tvorba]

4.4.4.2 Nastavení vzájemné replikace

Aby byla zajištěna stejnost obou doménových řadičů, je třeba nastavit vzájemnou replikaci mezi nimi. Výchozí hodnota je synchronizovat 1x za hodinu, ale pro vyšší efektivitu je třeba nastavit synchronizaci častější. Proto byla otevřena MMC konzole a přidán modul „Active Directory Sites and Services“, zvoleno „Sites“ – „Default-First-Site-Name“ – „LG-DC1“ – „NTDS Settings“, dvojklikem otevřeno nastavení automaticky generované replikace a zvoleno „Change schedule“. Zde bylo nastavení změněno z „Once per Hour“ na „Four Times per Hour“. Stejným způsobem byla změna provedena i u serveru LG-DC2 ve stejné nabídce. Po uložení se automaticky generovaná replikace změnila na ručně nastavenou replikaci, která se již bude provádět každých 15 minut. Oba doménové řadiče byly následně vypnuty a byl vytvořen kontrolní bod.

4.4.5 Instalace testovací klientské stanice

Aby bylo možné testovat uživatelské možnosti v průběhu úprav nastavení na serverech, vytvořil autor nový virtuální stroj. Jméno zvolil „CZ1V-1“ podle jmenné konvence firmy Linet. „CZ1“ značí, na které pobočce je stanice používána, „V“ značí, že se nejedná o pevný počítač „D“, nebo laptop „L“, ale o virtuální stanici. Číslo 1 na konci názvu značí pořadí, pro případ, že by bylo nutné vytvořit více testovacích stanic. Dále byla zvolena Generace 2, přiřazena paměť 2048 MB, připojen privátní „switch“, velikost disku omezena na 40 GB. Ze stránek DreamSpark [17] byl stažen operační systém „Windows 10 Education

64bit verze 1809“, který je určen pro koncové stanice. Soubor byl připojen do virtuální DVD mechaniky nově vytvořené stanice a po zapnutí stanice se z ní spustila instalace.

Jazyk byl ponechán anglický, v dalším kroku byl vložen licenční klíč získaný na webu DreamSpark [17], a ostatní kroky byly beze změny potvrzeny. Po nainstalování autor zvolil region Česká republika a rozložení klávesnice české, i anglické. Poté bylo potřeba stroj připojit k síti pomocí externího „switche“, pro aktivaci Windows a získání nejnovějších aktualizací. Zároveň byl stroj připojen k privátnímu „switchi“, aby mohl být později přidán do domény. V následujícím kroku byl vytvořen lokální účet „OEM“. Poté následovalo několik kroků pro nastavení soukromí, zjišťování polohy, personalizace hlasového psaní a další, jejichž charakteristika není předmětem této práce. Po zobrazení plochy byla ihned spuštěna instalace aktualizací, po jejímž dokončení byl odpojen externí switch a stanice restartována. Počítač byl přejmenován z výchozího názvu „DESKTOP-B8AO03P“ na „CZ1V-1“. Po dalším restartu počítač nešel přidat do domény, proto autor zjistil pomocí příkazovém řádku, že stanice nemá přiřazenou IP adresu. Proto zkontroloval nastavení DHCP na serveru LG-DC1 a následně znovu autorizoval neaktivní DHCP. Poté již počítač získal IP adresu 10.0.1.11 a bylo možné ho přidat do domény „linet-group.local“.

4.4.6 Vytvoření virtuálního sdíleného disku

Aby bylo možné efektivně kopírovat soubory na virtuální stanice, bylo potřeba vytvořit sdílený disk. Autor jej bude využívat pro kopírování databázových a instalačních souborů, aby s nimi dále mohl pracovat. V hlavním panelu Hyper-V bylo kliknuto na „New“ – „Hard disk“. Zde bylo na výběr ze tří druhů virtuálních disků:

- **VHD** – starší typ, který může mít kapacitu pouze 2040 GB
- **VHDX** – novější typ, který podporuje velikost až 64 TB, ale nelze jej použít u stanic se staršími operačními systémy než Windows 8.
- **VHD Set** – nejnovější typ, který ale slouží především pro zálohování skupin virtuálních stanic, které využívají virtuální disky. Tento formát je podporován pouze na operačních systémech Windows 10.

Pro potřeby testování byl zvolen typ VHDX, který je nejvhodnější pro potřeby, za kterými bude disk využíván. V dalším kroku byla volba typu virtuálního disku:

- **Pevná velikost** – nejvíce kapacitně náročný. Vhodný pro aplikace, které jsou kriticky závislé na tomto virtuálním disku. Disk po vytvoření zabírá definované místo na fyzickém disku.
- **Dynamické přírůstky** – šetří místo na disku. Vhodný pro aplikace, které na disku nejsou příliš závislé. Disk zabírá pouze místo, které je využito soubory na něm.
- **Diferenciální** – slouží pro vztah rodič-dítě s jiným diskem. Na disku „dítě“ je možné provádět změny bez ovlivnění disku „rodič“, takže je snadné a rychlé vrátit provedené změny. Všechny disky v tomto vztahu musí být stejného druhu (VHD nebo VHDX).

Disk nebude použit pro ukládání kriticky důležitých souborů, ale naopak bude potřebovat měnit dynamicky velikost disku v případě potřeby přenosu velkých souborů. Proto byl zvolen typ „Dynamické přírůstky“. V dalším kroku autor disk pojmenoval „LINET-GROUP“ a umístil ho na disk určený pro testovací prostředí.

4.4.6.1 Připojení disku k virtuálním stanicím

Aby bylo možné disk připojit k virtuální stanici, bylo potřeba ho nejprve inicializovat. Na fyzickém hostujícím počítači autor otevřel „Disk Management“, a již po spuštění systém sám nabídl inicializaci nově nalezeného disku. Autor nabídku potvrdil a spustil formátování disku. Při tomto procesu mu přiřadil název „LINET-GROUP“. Dále autor na fyzickém počítači vytvořil nového uživatele „\\Martin-PC\lg-drive“, který bude sloužit pouze pro připojování virtuálních stanic na tento sdílený disk. Ke všem stanicím byl připojen externí virtuální switch a následně k nim byl disk připojen pomocí cesty „\\Martin-PC\g“. Při odpojení externího switche disk na stanicích nebude dostupný.

4.4.7 Simulace struktury firmy v AD

Pomocí skriptů Powershell byla z reálného firemního prostředí vyexportovány data potřebná pro simulaci struktury firmy v AD. Následujícím skriptem byl vyexportován seznam všech organizačních jednotek se všemi podrobnostmi v Active Directory:

- Get-ADOrganizationalUnit -filter * -properties *

Pro získání organizačních a bezpečnostních skupin byl použit skript:

- Get-ADGroup -filter * -properties *

Seznam všech uživatelských účtů a jejich podrobností byl získán skriptem:

- Get-ADUser -filter * -properties *

Následující příkaz byl použit pro získání listu všech počítačů:

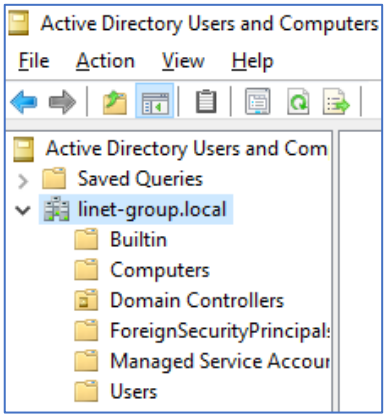
- Get-ADComputer -filter * -properties *

Každý ze seznamů byl vyexportován pomocí skriptu:

- Export-Csv -Path c:\install\DP\ADxx.csv

4.4.7.1 **Import organizačních jednotek**

Pro ověření funkčnosti skriptu byla zachycena struktura organizačních jednotek před importem.



Obrázek 17 - Struktura organizačních jednotek před importem [Vlastní tvorba]

V stanici LG-DC1 byla vytvořena složka C:/Install, do níž byl nakopírován soubor „ADOU.csv“ se strukturou organizačních jednotek, získaný PowerShell příkazem [Kapitola 4.4.7]. Byl spuštěn Windows PowerShell a následujícím příkazem byla struktura importována:

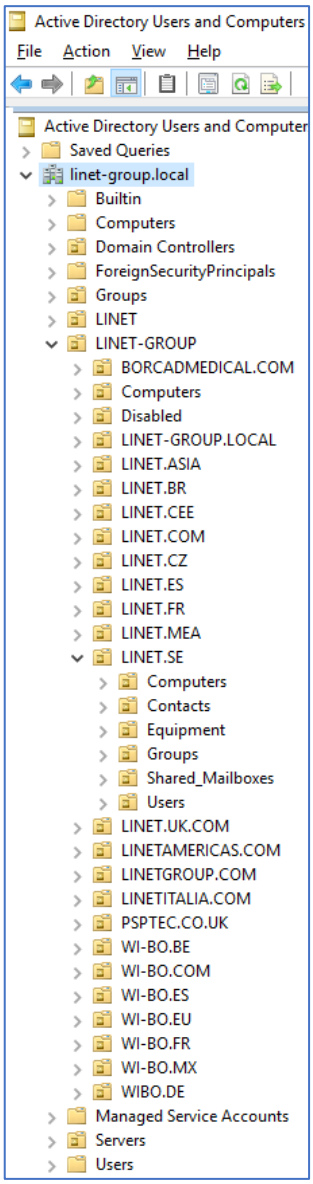
```powershell
$ous = Import-Csv -Path "C:\Install\ADOU.csv" -delimiter ";"


foreach ($ou in $ous)
{
    $ouname = $ou.Name
    $oudn = $ou.DistinguishedName

    New-ADOrganizationalUnit -Name $ouname -Path $oudn  -ManagedBy 'domain admins'
}
```

Obrázek 18 - Import OU [Vlastní tvorba]

Příkazem „$ous“ byla definována proměnná obsahující cestu k datovému souboru a pomocí „-delimiter“ byl definován oddělovač v CSV datovém souboru. Výchozím oddělovačem je totiž znak „ , “, ale kvůli výchozímu formátování exportovaných dat byl použit znak „ ; “. Cyklus „foreach“ slouží pro vytvoření nové organizační jednotky pro každý řádek zdrojového souboru. Pomocí parametrů „$ouname“ a „$oudn“ byly definovány název a umístění nově vytvářených organizačních jednotek na základě dat v zdrojovém souboru. Na konec byly pomocí příkazu „New-ADOrganizationalUnit“ s využitím definovaných parametrů vytvořeny jednotlivé skupiny.

Pro zachování přehlednosti bylo potřeba vymazat organizační jednotky, které nesouvisí s testovanou problematikou. Ve výchozím nastavení jsou složky chráněné proti nechtěnému smazání. Pro povolení bylo nastaveno zobrazení rozšířených možností, následně bylo kliknuto na kořenovou složku „linet-group.local“, v záložce „security“ bylo zvoleno „advanced“ a zde byl odstraněn první záznam „zakázat smazání všech potomků“. Poté již bylo možné nepotřebné organizační jednotky vymazat.

Výsledná struktura obsahuje složky LINET a LINET-GROUP, kde je jedna podsložka pro každou zemi, ve které je kancelář firmy. Každá z těchto podsložek obsahuje složky „Computer“, „Contacts“, „Equipment“, „Groups“. „Shared_Mailboxes“ a „Users“.



Obrázek 19 - Struktura organizačních jednotek po importu [Vlastní tvorba]

4.4.7.2 Import skupin oprávnění

Obdobným způsobem autor naimportoval skupiny oprávnění do testovacího prostředí. Vzhledem k tomu, že v reálné struktuře existuje 1044 různých skupin, se autor rozhodl naimportovat pouze 250 nejpoužívanějších skupin, které jsou pro účely testování dostačující. První skript byl upraven do následující podoby:

```powershell
$groups = Import-Csv -Path "C:\Install\ADG.csv" -delimiter ";"


foreach ($group in $groups)
{
    $groupname = $group.Name
    $groupdn = $group.DistinguishedName
    $groupcategory = $group.GroupCategory
    $groupScope = $group.GroupScope


    New-ADgroup -Name $groupname -Path $groupdn -GroupCategory
    $groupcategory -GroupScope $groupScope -ManagedBy 'domain admins'
}
```

Obrázek 20 - Import skupin oprávnění [Vlastní tvorba]

Význam jednotlivých příkazů je analogický s prvním skriptem, pouze s použitím „group“ na místo „ou“.

4.4.7.3 Import uživatelských účtů

Příkaz pro importování uživatelských účtů byl nejsložitější. Vzhledem k množství detailů, které uživatelské účty obsahují, nebylo využito proměnných, jako v předchozích případech, ale atributy byly navázány přímo na zdrojový soubor pomocí „$_.“. Aby mohly být účty aktivní, musí být u nich vyplněné heslo. Pro import hesla z CSV bylo nutné klasický text převést na bezpečný řetězec, až poté bylo možné hesla naimportovat. Členství uživatelů ve skupinách se pomocí tohoto skriptu nepodařilo přenést, pro případ tohoto testování to ale není potřeba. V případě nutnosti bude u vybraných účtů doplněno ručně.

```powershell
import-csv -path "C:\Install\ADU.csv" -delimiter ";" |

% {New-ADUser -GivenName $_.GivenName -Surname $_.Surname -Name
$_.Name -SamAccountName $_.SamAccountName -DisplayName
$_.DisplayName -Description $_.Description -Department
$_.Department -Path $_.Path -Enabled $True -AccountPassword
(ConvertTo-SecureString $_.AccountPassword -AsPlainText -force)
-PasswordNeverExpires $True}
```

Obrázek 21 - Import uživatelských účtů [Vlastní tvorba]

Aby se uživatelské účty bez administrátorského oprávnění mohly přihlásit na virtuální stanici, bylo nutné na serveru LG-DC1 v okně „Local Security Policy“ – „Security Settings“ – „Local Policies“ – „User Rights Assignment“ u položky „Allow log on through Remote Desktop Servicies“ přidat vedle administrátorů ještě „Everyone“. V reálném prostředí by se jednalo o bezpečnostní hrozbu, v případě testování ale není fungování firmy ohroženo.

4.4.7.4 **Ověření replikace na řadič LG-DC2**

Po dokončení importu databáze bylo ověřeno, zda jsou tyto data viditelná i na druhém, záložním serveru LG-DC2. Bylo zjištěno, že na tomto serveru je stále stará struktura a neobsahuje žádné nové účty či skupiny. Při spuštění replikace ručně pomocí okna „Sites and Services“ se zobrazila chybová hláška o neshodě dat mezi jednotlivými řadiči. Proto autor řadič degradoval z doménového řadiče, aby mohl být opět přidán. Degradování řadiče bylo možné v nabídce „Manage“ – „Remove Roles and Features“. Při odebírání role doménového řadiče byl autor upozorněn, že je nutné nejprve server ponížit, až poté bude možné roli odebrat. Po ponížení serveru proběhl restart, po němž již server nebyl součástí domény, přesto ale stále měl roli doménového řadiče. Proces odebrání role byl spuštěn znovu, tentokrát již proběhl úspěšně, protože server byl již ponížený.

Záložní server byl znovu přidán do domény a následně povýšení na doménový řadič proběhlo totožným způsobem, jako v předchozím případě. Tím byl problém s replikací, který byl způsoben tím, že záložní doménový řadič byl vypnutý při importování dat do hlavního řadiče, odstraněn. Simulace firemního prostředí byla dokončena.

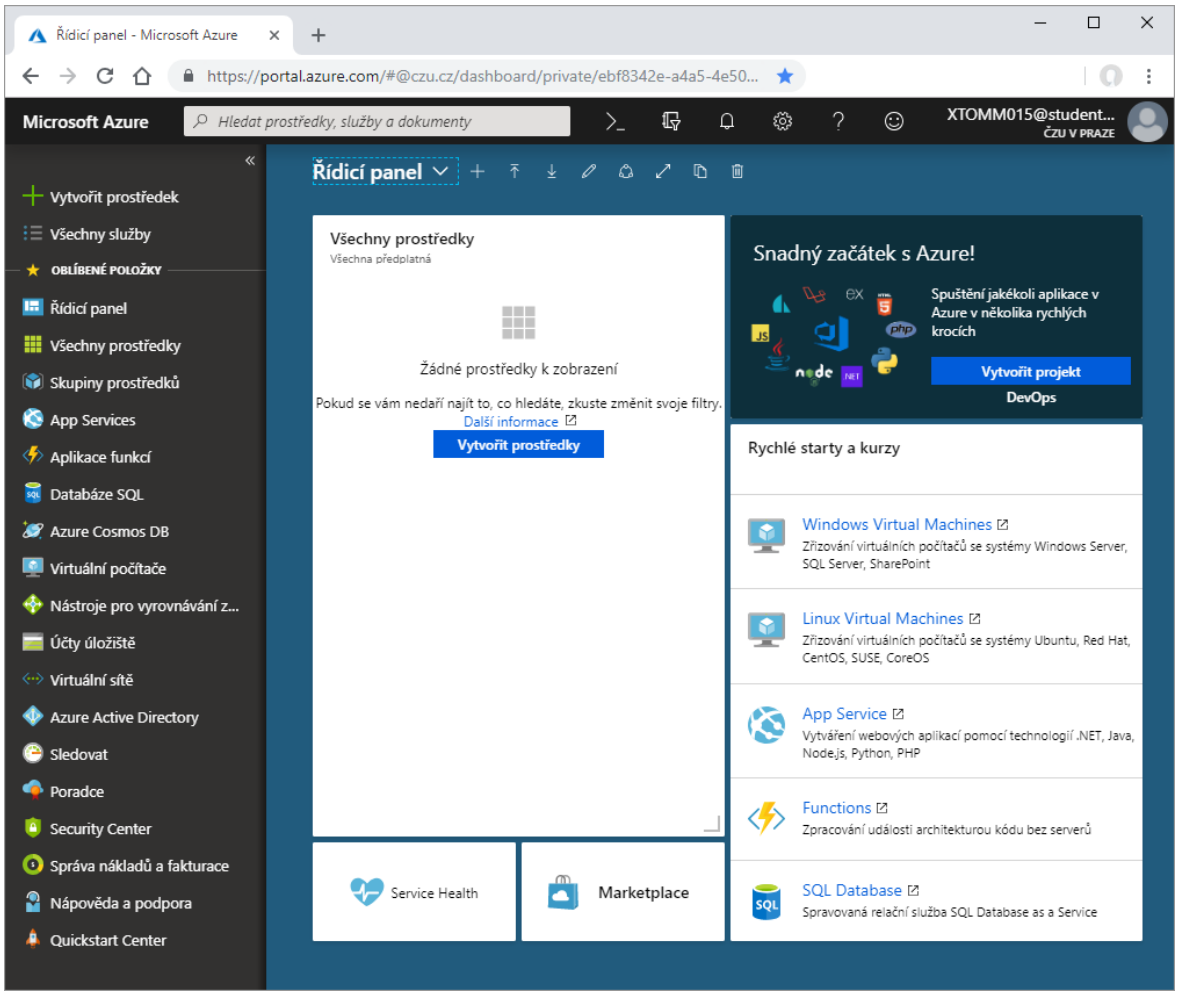
4.5 **Propojení AD a Mirosoft Azure AD**

Cloudová služba Azure AD nabízí rozšířené možnosti správy účtů [Kapitola 3.8]. Před propojením AD do MS Azure AD je potřeba ověřit, že jsou splněny všechny prerekvizity. První z nich je existence domény na serveru používajících operační systém Windows Server 2008 SP2, nebo novější. Tento bod je splněný. Druhou prerekvizitou je aktivní předplatné v Microsoft Azure. To zatím splněné není, autor se bude registraci a základnímu nastavení věnovat v následující kapitole. Posledním bodem je vlastnictví internetového doménového jména, vůči kterému se uživatelé budou ověřovat. Tento bod zatím také není splněný.

4.5.1 **Registrace do Microsoft Azure portálu**

Portál Microsoft DreamSpark poskytuje studentům vysokých škol stažení plných verzí Microsoft produktů pro studijní a osobní účely. Na tomto portálu je také nabízeno roční předplatné do Microsoft Azure s kreditem 100 dolarů, který je možné využít na pronájem virtuálních prostředků. Dále Microsoft nabízí velké množství online kurzů, aby se student

s portálem mohl naučit. Po potvrzení ročního předplatného je okamžitě možné se přihlásit do webového portálu https://portal.azure.com/ školním emailem.



Obrázek 22 - Portál Microsoft Azure [Vlastní tvorba]

4.5.2 Vytvoření nové kategorie v Azure AD

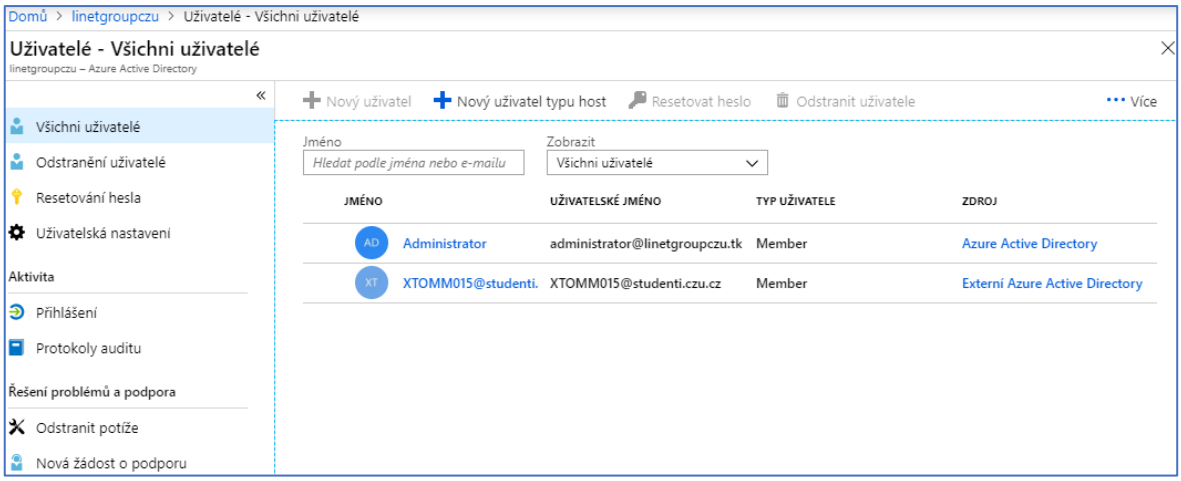
Kategorie reprezentuje naši organizaci a s ní spojené cloudové služby a nastavení. Pro její vytvoření bylo zvoleno „Vytvořit prostředek“ – „Identita“ – „Azure Active Directory“. Zde byl zvolen název organizace, i počáteční název domény „linetgroupczu“, „czu“ bylo za skutečný název domény přidáno, aby bylo testovací prostředí odlišeno od reálného prostředí firmy. Země byla zvolena „Česká republika“. Po potvrzení s v Azure Active Directory zobrazil přehled „linetgroupczu“, na místo výchozího přehledu, který se zobrazoval před vytvořením nové kategorie.

4.5.3 Propojení veřejné domény s Azure AD

Pro používání cloudových služeb je třeba mít zaregistrovanou doménu, která bude sloužit pro ověřování uživatelů. Proto byl vyhledán portál pro tvorbu domén zdarma https://my.freenom.com/, ve kterém byla vytvořena doména „linetgroupczu.tk“ pod školním účtem „xtomm015@studenti.czu.cz“. Po vytvoření byl nastaven DNS forwarding s údaji: typ = „TXT“, TLL = „3600“, target = „MS=ms81163017“. Tyto údaje byly zjištěny v portálu Azure v Azure Active Directory – „Názvy vlastních domén“, kam byla přidána doména „linetgroupczu.tk“. Po úspěšném nastavení byla doména ověřena a následně byl administrátor vyzván k propojení cloudové domény s lokální doménou.

4.5.4 Tvorba hlavního administrátorského účtu v Azure AD

V této kategorii byla otevřena nabídka „Azure AD“ – „Všichni uživatelé“, kde byl vytvořen hlavní administrátorský účet „Administrator“ s uživatelským jménem „administrator@linetgroupczu.tk“ a byla mu přiřazena role globálního administrátora. Při vytváření bylo automaticky vygenerováno heslo, které lze změnit až při prvním přihlášení. Proto byl v anonymním režimu prohlížeče otevřen portál „portal.azure.com“, do něj byl přihlášen nově vytvořený účet pomocí vygenerovaného hesla a po přihlášení byl autor vyzván ke změně, kde vygenerované heslo změnil na obecné administrátorské heslo.



Obrázek 23 - Přehled uživatelů Azure AD [Vlastní tvorba]

4.5.5 Instalace Azure AD Connect

Nyní jsou splněny všechny 3 prerekvizity pro propojení lokálního AD do Azure AD. Ze stránek Microsoftu [18] byl stažen instalační soubor pro Azure AD Connect a byl nakopírován na sdílený disk. Z něho byla na serveru LG-DC1 spuštěna instalace. Na začátku procesu byl autor upozorněn, že při použití expresního nastavení budou provedeny tyto kroky:

- konfigurace synchronizace identit v současném AD lese LINET-GROUP
- konfigurace zašifrované synchronizace hesel mezi lokálním AD a Azure AD
- spuštění synchronizace
- synchronizace všech atributů
- povolení automatických upgradů

Bylo použito toto expresní nastavení. V dalším kroku byly vyplněny kredence globálního administrátora Azure AD: „administrator@linetgroupczu.tk“, v následujícím kroku byly vyplněny kredence administrátora lokálního AD: „LINET-GROUP.LOCAL\administrator“.

4.5.5.1 Změna UPN

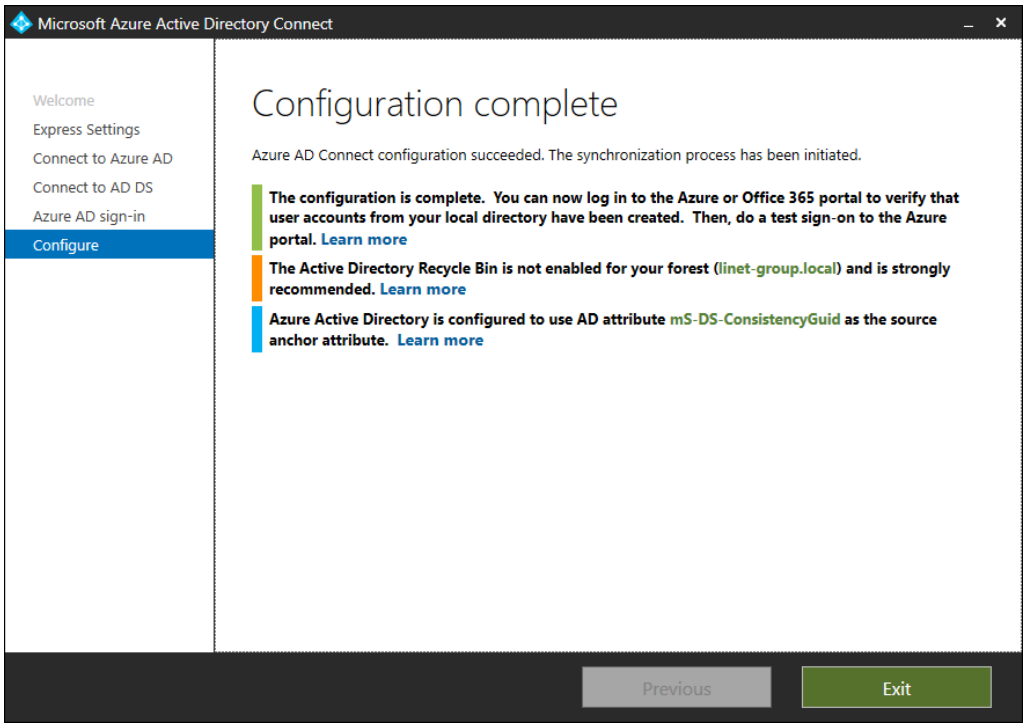
Poté byl autor upozorněn na nutnost souhlasu UPN (user principal name) mezi lokálním AD a Azure AD. Aby nedošlo ke konfliktu testovacího prostředí a reálného prostředí firmy, je nutné změnit UPN testovacího prostředí z „linet-group.local“ na „linetgroupczu.tk“. To bylo provedeno na serveru LG-DC1 v panelu „Active Directory Domains and Trusts“, pravým kliknutím na kořen stromu a zvolením možností bylo otevřeno okno pro přidání dalšího UPN. Zde bylo vyplněno „linetgroupczu.tk“. Pomocí následujícího příkazu Powershell bylo toto UPN nastaveno u všech uživatelů v doméně.

```
1  Get-ADUser -Filter * -Properties userPrincipalName |
2  foreach { Set-ADUser $_ -UserPrincipalName ("{0}@{1}" -f $_.SamAccountName,"linetgroupczu.tk")}
```

Obrázek 24 - Nastavení UPN [Vlastní tvorba]

Poté bylo ověřeno, že změna byla úspěšně replikována i na druhý řadič „LG-DC2“. V instalaci „Azure AD Connect“ byla potvrzena nabídka existujících sufixů a spuštěna instalace doplňku.

Během instalace byla nainstalována lokální databáze: „Microsoft SQL Server 2012 Express“ a vše úspěšně nakonfigurováno.



Obrázek 25 - Konfigurace Azure AD Connect (Zdroj: Vlastní zpracování)

Microsoft důrazně doporučuje povolit v Active Directory odpadkový koš pro vrácení případných nechtěných změn. Povolení je možní v panelu Administrative Center po zvolení domény. Při povolování byl autor upozorněn, že odpadkový koš již nelze nikdy odebrat.

Následně bylo ověřeno, že se již lze přihlásit do portálu Azure pomocí testovacího účtu v lokálním AD: „martin.toman@linetgrouczu.tk“ za použití synchronizovaného hesla definovaného v lokálním AD.

4.5.6 Omezení synchronizace pouze některých OU

Do cloudového AD není potřeba synchronizovat všechny organizační jednotky, například účty externistů, servisní účty a další. Omezení synchronizovaných složek je možné v nastavení aplikace „Azure AD Connect“ na serveru LG-DC1. V nabídce „další úkoly“ bylo zvoleno „přizpůsobit možnosti synchronizace“. Zde bylo přepnuto ze „synchronizovat celou doménu“ na „synchronizovat pouze zvolené OU“. Všechny OU „External“ byly

odznačeny a konfigurace potvrzena. Všichni uživatelé, kteří byli obsaženi v těchto složkách se v Azure přesunuly do složky „odstranění uživatelé“.

4.5.7 Manuální synchronizace

V případě provedení větších změn a potřeby ověření těchto změn v Azure AD, je třeba spustit synchronizaci ručně. To lze provést pomocí Powershell příkazů:

```
1   Import-Module ADSync
2   Start-ADSyncSyncCycle -PolicyType Initial
```

Obrázek 26 - Spuštění plné synchronizace [Vlastní tvorba]

V případě problémů se synchronizací je nutné přidat účet použitý pro spuštění služby synchronizace do Group Policy objektu „Log on as a service“, stejně jako v [4.7.1.2]

4.6 Samoobslužný reset hesla v Azure AD

Před povolením možnosti resetu hesla online pomocí Microsoft Azure byly změněny všechny emailové adresy uživatelů ze skutečných na testovací, s doménou @linetgroupczu.tk, aby nedošlo ke kontaktování skutečných uživatelů. K tomu byl využit Powershell příkaz:

```
1   Import-Module ActiveDirectory
2   Get-ADUser -Filter * | ForEach-Object { Set-ADUser -EmailAddress
3   ($_.samaccountname + '@linetgroupczu.tk') -Identity $_ }
```

Obrázek 27 - Hromadná změna emailových adres [Vlastní tvorba]

V doméně byla vytvořena skupina „Password_reset“ a do ní přidáno 5 testovacích uživatelských účtů, kterým bylo vyplněno mobilní telefonní číslo, směřující na mobil autora, aby mohla být otestována metoda ověřování přes mobilní telefon.

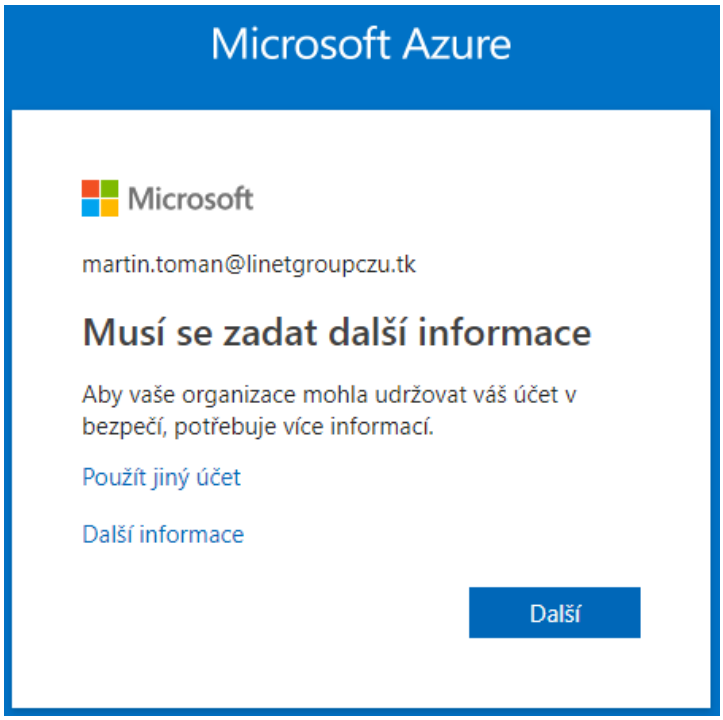
Povolení samoobslužného resetu hesla je možné v MS Azure v nabídce: „uživatelé“ – „Resetování hesla“ – „Aktivovat“. Aby bylo možné funkci aktivovat, je vyžadována Azure licence Premium, která není obsažena ve zkušební verzi. Licenci „Azure AD Premium P2“ je ale možné získat na 30 dní zdarma s licencí pro 100 uživatelů, a licenci Enterprise Mobility + Security E5“, která obsahuje také licenci Premium P2, je možné získat zdarma na 90 dní pro 250 uživatelů. Byla aktivována druhá licence s delší platností.

V portálu Azure v kategorii „Resetování hesla“ – „Metody ověřování“ bylo nastaveno ověřování pomocí E-mailu, mobilního telefonu a 3 bezpečnostních otázek, k ověření stačí 1 ověřovací metoda. Poté bylo resetování hesla povoleno AD skupině „Password_reset“.

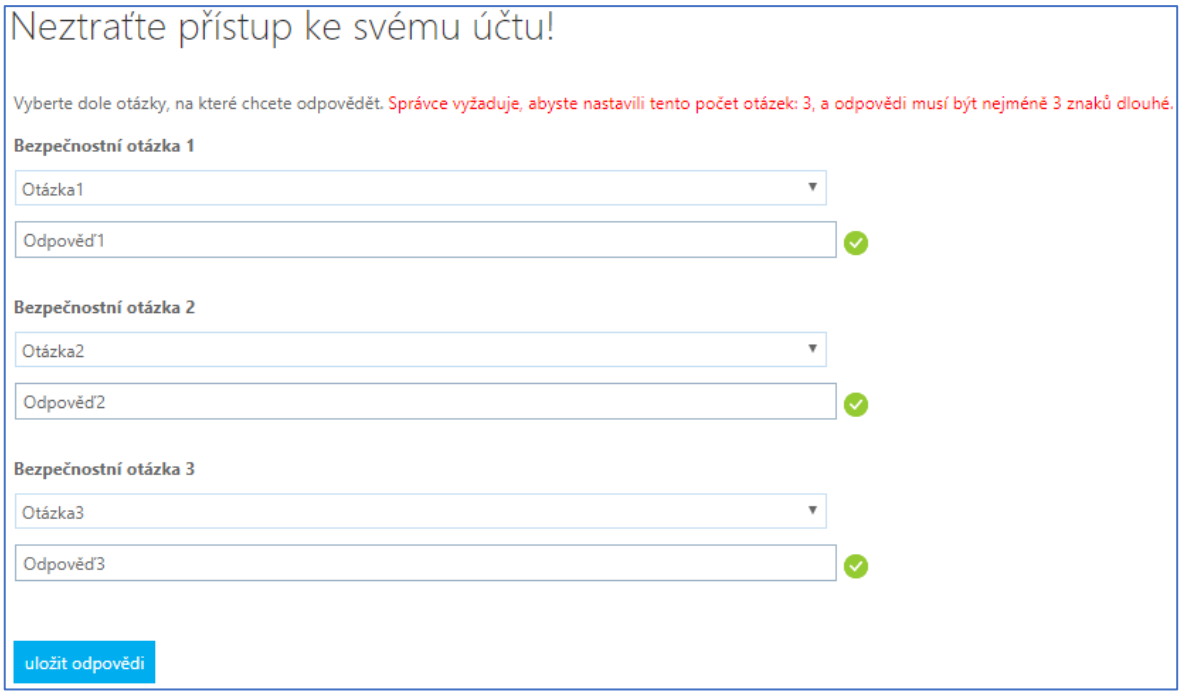
Aby se heslo resetované pomocí portálu Azure propsalo i do lokálního AD, je nutné změnit konfiguraci aplikace „Azure AD Connect“. Po jejím spuštění bylo zvoleno „Další úkoly“ - „Přizpůsobit možnosti synchronizace“ – „Volitelné funkce“ – zde bylo zvoleno „Zpětný zápis hesla“ a průvodce dokončen.

4.6.1 Testování samoobslužného resetu hesla

Po přihlášení do webového portálu Azure pomocí testovacího účtu s právy běžného uživatele: „martin.toman@linetgroupczu.tk“ byl autor vyzván k vyplnění bezpečnostních otázek.

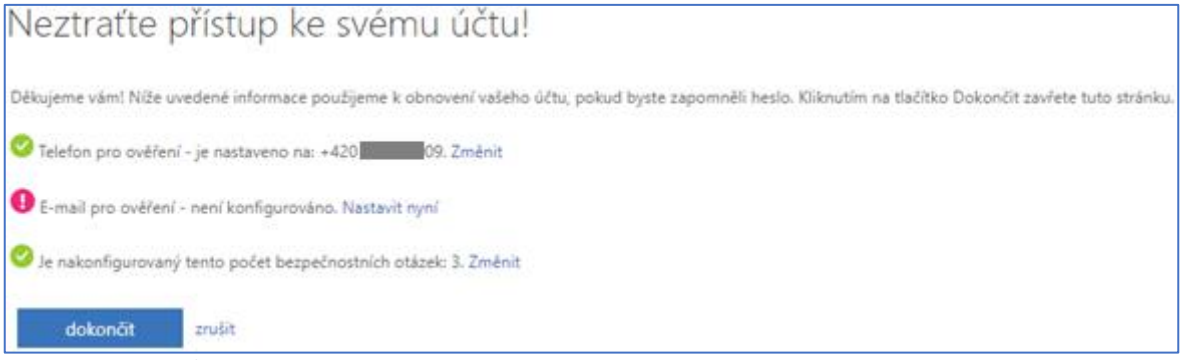


Obrázek 28 - Doplnění informací k účtu [Vlastní tvorba]



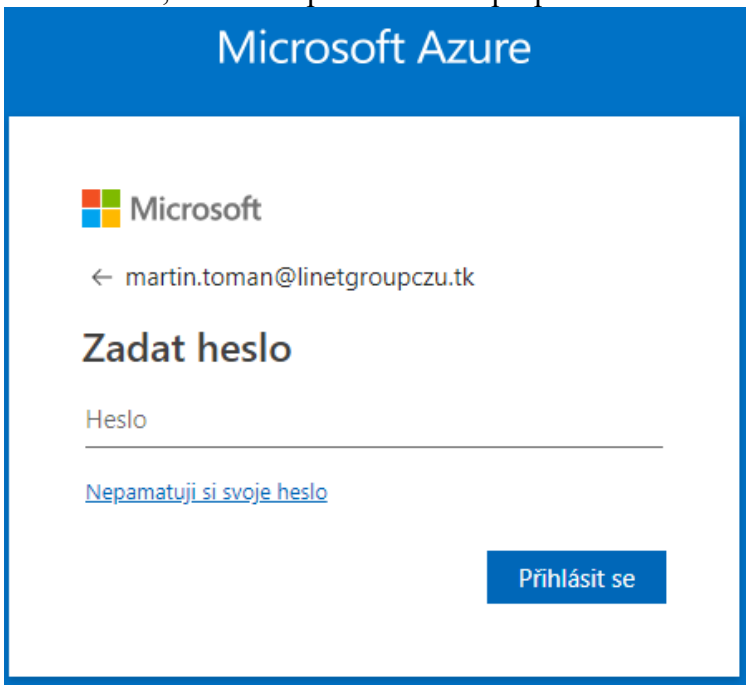
Obrázek 29 - Vyplnění bezpečnostních otázek [Vlastní tvorba]

Dále měl možnost změnit telefon a email pro ověřování. Email nebyl v tomto testovacím prostředí nakonfigurován, proto není dostupný pro ověření.

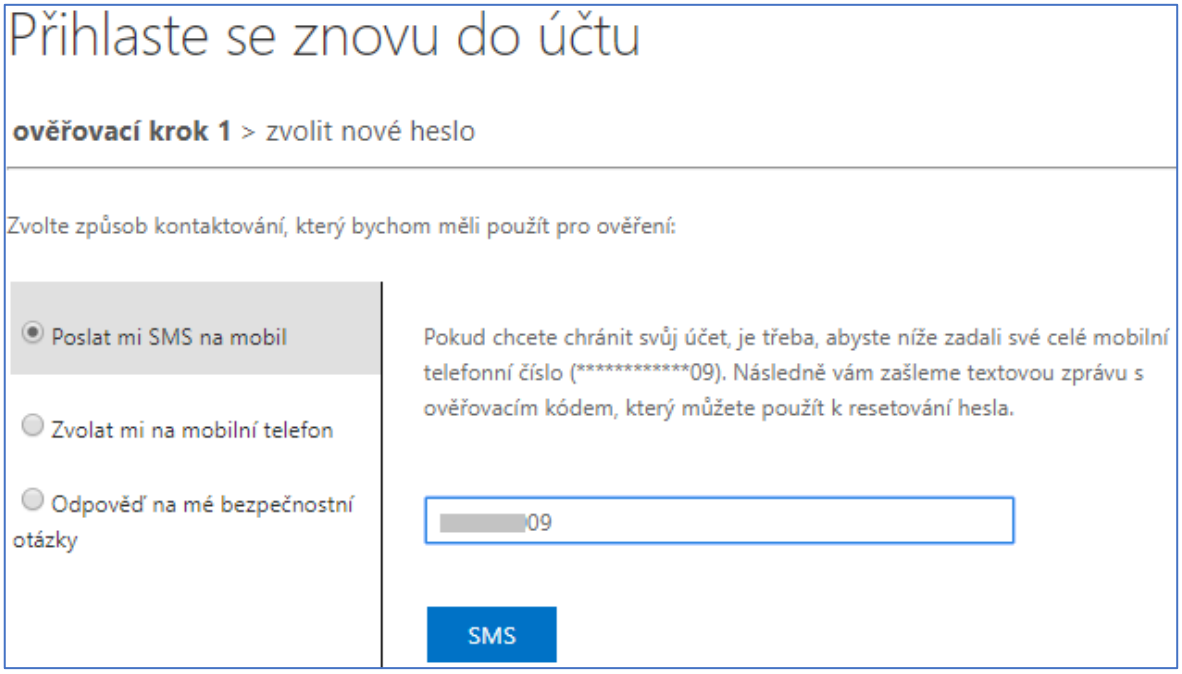


Obrázek 30 - Způsoby ověření [Vlastní tvorba]

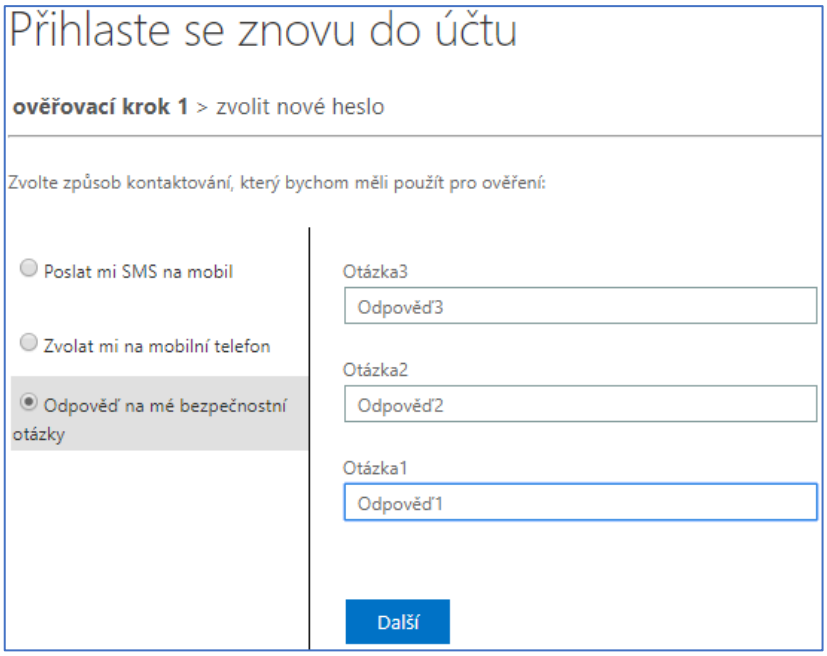
Při přihlašování do Azure portálu je možné kliknout na „Nepamatuji si svoje heslo“, tím se otevře nabídka s možnostmi pro ověření. Po úspěšném ověření dojde ke změně hesla, která se z portálu Azure propíše i do lokálního AD.



Obrázek 31 - Vyvolání nabídky na reset hesla [Vlastní tvorba]

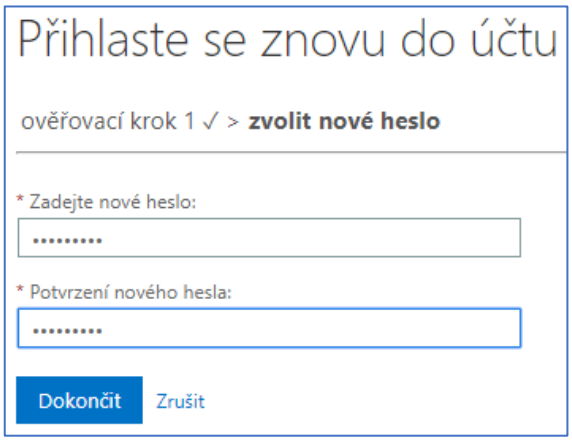


Obrázek 32 - Využití SMS na mobil [Vlastní tvorba]



Obrázek 33 - Využití bezpečnostních otázek [Vlastní tvorba]

Je možné definovat vlastní počet otázek s libovolným obsahem. Pro účely testování byly použity pouze zástupné otázky.



Obrázek 34 - Volba nového hesla [Vlastní tvorba]

4.6.2 Výsledek testování

Pomocí virtuálního testovacího uživatelského počítače bylo ověřeno, že heslo je možné úspěšně změnit všemi nabízenými způsoby a poté jej lze použít pro přihlášení do počítače. Heslo se tedy propisuje z Azure AD do místního AD. Způsob je velmi intuitivní, nabízí širokou škálu nastavení a je možné jej použít kdekoliv s přístupem k internetu.

4.7 MIM

Příprava prerekvizit pro instalaci Microsoft Identity Manager se skládá z následujících kroků: příprava domény, instalace virtuálního stroje, instalace SQL Server a SharePoint Server.

4.7.1 Příprava domény na instalaci MIM

V AD bylo vytvořeno několik servisních účtů: „MIMInstall“, „MIMMA“, „MIMService“, „MIMSync“, „MIMSSPR“, „SharePoint“ a „SqlServer“, a několik skupin: „MIMSyncAdmins“, do které byly přidány účty „Administrator“, „MIMService“ a „MIMInstall“, dále skupiny „MIMSyncBrowse“, „MIMSyncJoiners“, „MIMSyncOperators“ a „MIMSyncPasswordReset“. Pro to byl využit následující skript:

```
New-ADGroup -name MIMSyncAdmins -GroupCategory Security -GroupScope Global -SamAccountName MIMSyncAdmins
New-ADGroup -name MIMSyncOperators -GroupCategory Security -GroupScope Global -SamAccountName MIMSyncOperators
New-ADGroup -name MIMSyncJoiners -GroupCategory Security -GroupScope Global -SamAccountName MIMSyncJoiners
New-ADGroup -name MIMSyncBrowse -GroupCategory Security -GroupScope Global -SamAccountName MIMSyncBrowse
New-ADGroup -name MIMSyncPasswordReset -GroupCategory Security -GroupScope Global -SamAccountName MIMSyncPasswordReset
Add-ADGroupMember -identity MIMSyncAdmins -Members Administrator
Add-ADGroupmember -identity MIMSyncAdmins -Members MIMService
Add-ADGroupmember -identity MIMSyncAdmins -Members MIMInstall
```

Obrázek 35 - Tvorba servisních skupin [19]

Tyto prostředky budou později využívány při nastavován MIM.

Dále byly na doménovém řadiči zadány následující příkazy do příkazového řádku pro nastavení SPN [Kapitola **Chyba! Nenalezen zdroj odkazů.**]:

setspn -S http/LG-MIM.linetgroupczu.tk Linet-Group\mimpool

setspn -S http/LG-MIM Linet-Group\mimpool

setspn -S http/passwordreset.linetgroupczu.tk Linet-Group\mimsspr

setspn -S http/passwordregistration.linetgroupczu.tk Linet-Group\mimsspr

setspn -S FIMService/LG-MIM.linetgroupczu.tk Linet-Group\MIMService

setspn -S FIMService/corpservice.linetgroupczu.tk Linet-Group\MIMService

4.7.1.1 Úprava DNS

V DNS Manageru byla vytvořená nová „Forward Lookup Zone“ se jménem „linetgroupczu.tk“, což je webová stránka, vůči které se uživatelé budou ověřovat. Dále bylo nutné vytvořit „Reverse Lookup Zone“ s IP adresou rozsahu „10.0.1“. Poté mohly být do

DNS přidány 3 A záznamy: „mim.linetgroupczu.tk“, „passwordreset.linetgroupczu.tk“ a „passwordregistration.linetgroupczu.tk“, všechny tři směřující na IP adresu serveru „LG-MIM“: 10.0.1.3. Stejné záznamy byly přidány i do zóny „linet-group.local“.

4.7.1.2 **Úprava GPO**

Následně bylo upraveno GPO následujícím způsobem: „Group Policy Management“ – „Forest: linet-group.local“ – „Domains“ – „linet-group.local“ – „Default Domain Policy“ kliknuto pravým tlačítkem a zvoleno „Edit…“. V tomto editoru bylo zvoleno: „Computer Configuration“ – „Policies“ – „Windows Settings“ – „Security Settings“ – „Local Policies“ – „User Rights Assignemnt“, zde otevřeno nastavení: „Log on as a service“ a sem přidáno všech 5 servisních účtů vytvořených dříve [Kapitola 4.7.1], a dále do nastavení „Deny access to this computer from the network“ a „Deny log on locally“ přidány servisní účty „MIMservice“ a „MIMSync“.

4.7.2 **Instalace serveru LG-MIM**

Na fyzické testovací stanici byl v Hyper-V vytvořen nový virtuální stroj „LG-MIM“, Generace 2, přiřazeno 4096 MB dynamické paměti, připojen na externí switch pro instalaci aktualizací, velikost disku omezena na 40 GB, za instalační médium zvolen .iso soubor s verzí Windows Server 2016. Po zapnutí virtuálního stroje byla spuštěna instalace operačního systému, po které byl stroj přejmenován na „LG-MIM“, po nainstalování aktualizací byl odpojen od externího switche a připojen na privátní switch, aby byl ve stejné síti jako ostatní virtuální stroje. Následně mu byla přidělena statická IP adresa 10.0.1.3, maska podsítě 255.255.255.0 a výchozí brána a DNS server 10.0.1.1. Poté byl přidán do domény „linet-group.local“. Aby měl tento virtuální stroj dostatek prostředků, byla maximálně využitelná paměť pro stroje LG-DC1 a LG-DC2 omezena z 4096 MB na 2048 MB, což je pro testovací prostředí dostatečné, a v případě potřeby může být později opět navýšena.

4.7.3 Příprava serveru LG-MIM na instalaci Microsoft Identity Manager

Před začátkem dalšího kroku byly aktualizovány lokální „group policy“ pomocí příkazu: „gpupdate /force /target:computer“. Další nezbytnou částí přípravy je přidělení několika rolí a funkcí serveru „LG-MIM“. Ty byly přidány pomocí následujícího Powershell příkazu:

```
import-module ServerManager

Install-WindowsFeature Web-WebServer,Net-Framework-Features,rsat-ad-
powershell,Web-Mgmt-Tools,Windows-Identity-Foundation,Server-Media-Foundation,Xps-
Viewer -includeallsubfeature -restart -source d:\sources\SxS
```

Obrázek 36 - Přidání potřebných rolí a funkcí [20]

Dále bylo třeba upravit IIS [Kapitola 0] Windows Authentication mode. K tomu byly využity 3 Powershell příkazy zobrazené v následujícím obrázku:

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> iisreset /STOP

Attempting stop...
Internet services successfully stopped
PS C:\Windows\system32> C:\Windows\System32\inetsrv\appcmd.exe unlock config /section:windowsAuthentication -commit:apphost
Unlocked section "system.webServer/security/authentication/windowsAuthentication" at configuration path "MACHINE/WEBROOT/APPHOST".
PS C:\Windows\system32> iisreset /START

Attempting start...
Internet services successfully started
PS C:\Windows\system32>
```

Obrázek 37 - Změna IIS Windows Authentication mode [Vlastní tvorba]

4.7.3.1 Instalace SQL Server 2017 Enterprise

Pomocí portálu Micorosft Dreamspark [17] byl stažen instalační .ISO soubor pro instalaci SQL Server 2017 Enterprise. Instalační soubor byl připojen do virtuální mechaniky virtuálního počítače „LG-MIM“ a z té byla spuštěna instalace. V instalačním průvodci byla zvolena možnost „Instalation“ – „New SLQ Server stand-alone installation“. Po načtení instalace byl, díky stažení z portálu Dreamspark, již předvyplněný licenční klíč. Při kontrole instalačních pravidel byl autor upozorněn na aktivní Windows Firewall. Aby mohlo být bez chyby pokračováno, byl Firewall vypnut. Stroj není připojen k internetu, takže se nejedná o bezpečnostní riziko. V dalším kroku byl výběr instalovaných komponent. Potřebné komponenty jsou: „Database Engine Services“ a „Full-Text and Semantic Extractions for Search“ [21]. Poté byly změněny servisní účty pro SQL Server Agent na „NT AUTORITY\Network Service“ a nastaven z manuálního na automatické spuštění a pro

„SQL Server Database Engine“ na dříve vytvořený „LINET-GROUP\SQLServer“ s výchozím administrátorským heslem, a byla přidána výchozí skupina „Administrators“ mezi administrátory SQL serveru. Následně byla již spuštěna samotná instalace, která byla dokončena s výchozím nastavením.

Po instalaci bylo zjištěno, že instalovaná verze nenabízí instalaci doplňku „SQL Server Management Tools“ tak, jako tomu bylo u předchozích verzí. Tu bylo potřeba stáhnout ze stránek Microsoftu [22] a nainstalovat zvlášť. Stažený soubor byl nakopírován do virtuálního stroje „LG-MIM“ prostřednictvím sdíleného disku. Po spuštění instalace nebyla možnost něco změnit, „Management Studio“ se, po potvrzení licenčních podmínek, začalo instalovat. Po dokončení instalace bylo „Management Studio“ spuštěno a připojeno na SQL server „LG-MIM“. Ve výchozím nastavení má SQL server neomezené množství paměti, které nikdy neuvolní, a tím dojde brzy k přetížení serveru. Pro omezení množství paměti serveru bylo kliknuto pravým tlačítkem na kořen struktury, zvoleno nastavení serveru, a zde v záložce „Memory“ byla nastavena maximální paměť serveru na 2048 MB, což je polovina celkové paměti přidělené serveru.

4.7.3.2 **Instalace Sharepoint Server 2019 Enterprise**

Instalační soubor pro instalaci Sharepoint serveru byl stažen ze zdrojových stránek Dreamspark [17] a připojen k serveru „LG-MIM“ do virtuální mechaniky. Jako první byla spuštěna instalace „PrerequisiteInstaller.exe“, což zajistí přítomnost všech potřebných doplňků. Stroj musí být během této instalace připojen k internetu, což bylo zajištěno připojením externího virtuálního switche. V průběhu instalace bylo potřeba stroj restartovat a po restartu instalace pokračovala dál. Po dokončení instalace prerekvizit byla spuštěna instalace samotného Sharepoint serveru pomocí souboru „setup.exe“. Po dokončení instalace bylo nutné stroj restartovat a následně byla spuštěna konfigurace. Na jejím začátku byl autor upozorněn, že během procesu bude potřeba restartovat služby: „IIS“, „Služba pro správu SharePointu“ a „Služba Časovač služby SharePoint“. V testovacím prostředí se nejedná o žádné nebezpeční, proto byl restart služeb potvrzen. Poté byla zvolena volba „Vytvořit novou serverovou farmu“. Databázový server byl nastaven: „LG-MIM“ a účet pro přístup k databázi: „linet-group\SharePoint“. Poté byla učena role serveru na „Front-end“ a zadáno číslo portu „999“ pro webovou aplikaci „Centrální správy SharePoint“. Následně

byla spuštěna instalace, po jejímž dokončení byl autor upozorněn, že webové rozhraní Sharepoint je dostupné na adrese: http://lg-mim:999/.

Aby mohlo být webové rozhraní otevřeno, musela být stránka přidána do důvěryhodných stránek, jinak byla z bezpečnostních důvodů blokována. Po její otevření bylo nutné se přihlásit pomocí účtu „linet-group\administrator“. Poté byl otevřen „Průvodce konfigurací“, kde bylo potvrzeno, že chceme server nastavit pomocí průvodce, a ne ručně. V prvním kroku průvodce byl zvolen servisní účet „linet-group\SharePoint“ pro správu, druhý krok byl přeskočen, bude nastaveno později.

Dále bylo třeba odstranit výchozí webovou aplikaci, aby následně mohla být vytvořena nová s korektním nastavením. To bylo možné v nabídce „Správa aplikací“ – „Spravovat webové aplikace“, kde byla označena „SharePoint – 80“ a smazána. Poté byla pomocí SharePoint Management Shell vytvořena nová webová aplikace příkazem:

```
$dbManagedAccount = Get-SPManagedAccount -Identity linet-group\mimpool

New-SpWebApplication -Name "MIM Portal" -ApplicationPool "MIMAppPool" -
ApplicationPoolAccount $dbManagedAccount -AuthenticationMethod "Kerberos" -Port
80 -URL http://mim.linetgroupczu.tk
```

Obrázek 38 - Tvorba webové aplikace [Vlastní tvorba]

Po vytvoření je potřeba aplikaci správně nastavit pomocí několika po sobě jdoucích příkazů:

```
PS C:\Users\administrator.LINET-GROUP> $web = Get-SPWebApplication http://LG-MIM.linet-group.local
PS C:\Users\administrator.LINET-GROUP> $web.CompatibilityRange

MaxCompatibilityLevel MinCompatibilityLevel DefaultCompatibilityLevel Singular
--------------------- --------------------- ------------------------ --------
                   15                    15                       15     True

PS C:\Users\administrator.LINET-GROUP>  $t = Get-SPWebTemplate -compatibilityLevel 15 -Identity "STS#1"
PS C:\Users\administrator.LINET-GROUP> New-SPSite -Url $web.Url -Template $t -OwnerAlias linet-group\administrator -CompatibilityLevel 15 -Name "MIM Portal"

Url                                            CompatibilityLevel
---                                            ------------------
http://lg-mim.linet-group.local                15
PS C:\Users\administrator.LINET-GROUP> $s = SpSite($web.Url)
PS C:\Users\administrator.LINET-GROUP> $s.CompatibilityLevel
15
PS C:\Users\administrator.LINET-GROUP> $contentService = [Microsoft.SharePoint.Administration.SPWebService]::ContentService;
PS C:\Users\administrator.LINET-GROUP> $contentService.ViewStateOnServer = $false;
PS C:\Users\administrator.LINET-GROUP> $contentService.Update();
PS C:\Users\administrator.LINET-GROUP> Get-SPTimerJob hourly-all-sptimerservice-health-analysis-job | disable-SPTimerJob
```

Obrázek 39 - Nastavení webové aplikace [Vlastní tvorba]

Když všechny příkazy proběhly úspěšně a bez chyby, bylo v portálu Správa webových aplikací ověřeno, že se webová aplikace „MIM Portal“ skutečně vytvořila. Poté bylo ve „Správě aplikací“ zvoleno „Konfigurovat mapování alternativních adres URL“ a zde byla přidána do kolekce „MIM Portal“ interní adresa „http://LG-MIM“. Následně bylo ověřeno, že lze otevřít webovou aplikaci na adrese „http://LG-MIM“ a administrativní část na „http://LG-MIM:999“.

4.7.4 Instalace Microsoft Identity Manager 2016 SP1

Instalační soubor pro instalaci MIM 2016 SP1 bohužel není dostupný na studentském portálu Dreamspark, proto byla stažena evaluační verze funkční 180 dní z oficiálních stránek Microsoftu [23]. Soubor byl standardně připojen do virtální mechaniky stanice „LG-MIM“.

4.7.4.1 Instalace služby synchronizace

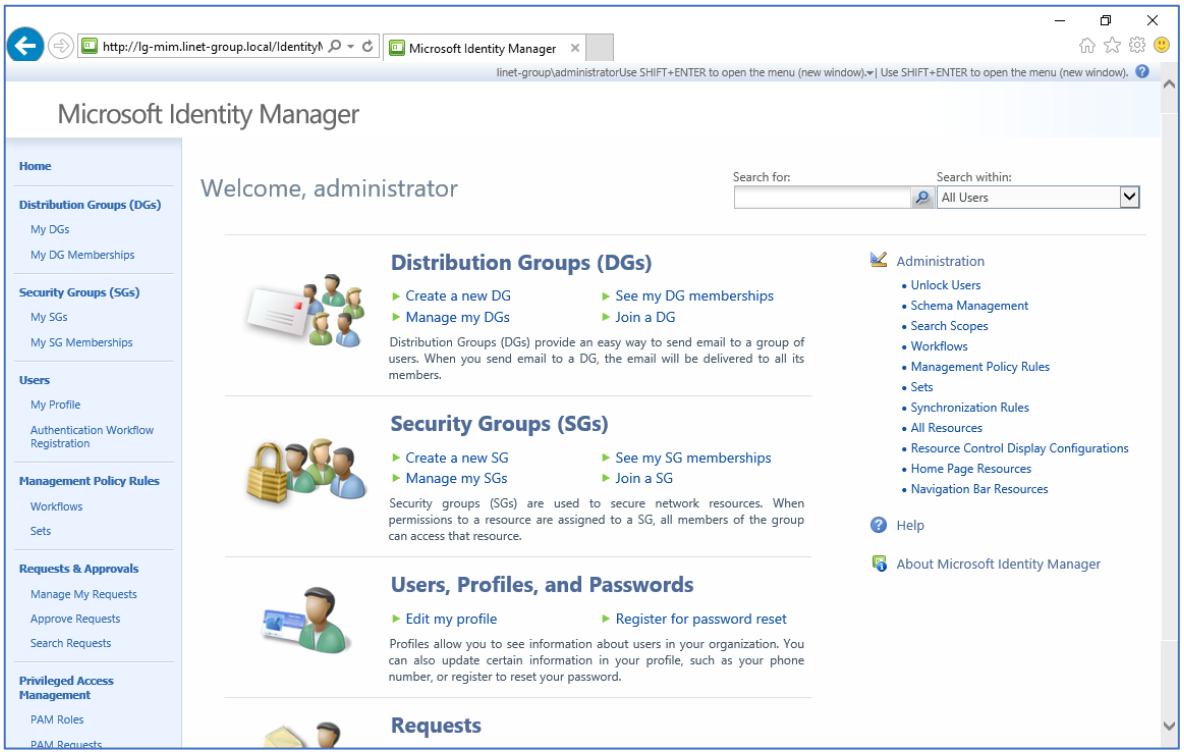
Na disku byl, ve složce „Synchronization Service“, spuštěn soubor „Synchronization Service.msi“. SQL databáze je nainstalována na tomto stroji, bylo tedy ponecháno výchozí nastavení. V dalším kroku byly zadány kredence servisního účtu „MIMsync“ a doména „LINET-GROUP“. V dalším kroku byly výchozí hodnoty servisních skupin s „FIMSync*“ na dříve vytvořené „LINET-GROUP\MIMSync*“. Poslední skupina obsahovala výchozí hodnotu „*PasswordSet“, ale vytvořená skupina se jmenovala „*PasswordReset“. Bylo tedy potřeba výchozí hodnotu opravit. Následně bylo zvoleno povolení pravidel v bráně firewall. Poté byla spuštěna instalace, po jejímž dokončení byla na stanici dostupná aplikace „Synchronization service“. Bylo zjištěno, že služba, spjatá se synchronizací Identity Manageru nemohla být spuštěna, kvůli nedostatečným právům účtu „MIMSync“. Proto byl tento účet v nastavení služeb změněn na „Administrator“. Poté již služba spustit šla a bylo možné i otevřít aplikaci „Synchronization service“.

4.7.4.2 Instalace portálu

Dalším krokem je instalace „Service and Portal“ pomocí „D:/Service and Portal/setup.exe“. Při volbě komponent bylo ponecháno výchozí nastavení. V dalším kroku při tvorbě databáze byl opraven výchozí název „FIMService“ na „MIMService. Název „FIM“ pochází z předchozí verze tohoto programu a Microsoft zde ponechal chybu. V následujícím kroku je třeba vyplnit mail server. Ten zatím neexistuje, přesto je ale nutné něco vyplnit, proto byl vyplněn název serveru „LG-MIM.linet-group.local“. V dalším kroku byla ponechána výchozí hodnota pro vygenerování vlastního certifikátu. Poté byl vyplněn servisní účet „MIMService“ a jeho neexistující emailová adresa „MIMservice@linet-group.local“, bez níž by nebylo možné pokračovat. Následně byl vyplněn účet „linet-group\MIMSync“ do kolonky „MIM Management Aget Account“ a „LG-MIM“ za adresu

„MIM Service Server“. Adresa Sharepoint kolekce byla nastavena na „http://LG-MIM.linet-group.local“. Adresa registračního portálu nebyla vyplněna. Bylo zaškrtnuto, aby uživatelům byly přiděleny práva na přístup do MIM portálu.

Další částí je konfigurace portálu pro registraci hesla, kam byly vyplněny následující údaje: Název účtu „Linet-group\administrator“, host name: „passwordregistration.linet-group.local“ a port „80“. Podobně byla nastavena konfigurace portálu pro reset hesla, která se lišila pouze v Host name: „passwordreset.linet-group.local“. Poté již byla spuštěna instalace MIM portálu. Instalace byla v průběhu přerušena s chybou. Po důkladném prověření bylo zjištěno, že na vině je česká verze Sharepoint serveru, proto byl stažen anglický jazykový balíček a byl zpětně doinstalován. Poté byla instalace znovu spuštěna a tentokrát dokončena úspěšně. Úspěšnost instalace byla ověřena, po restartu počítače, otevřením webové stránky: „http://lg-mim.linet-group.local/IdentityManagement“.



Obrázek 40 - Rozhraní MIM [Vlastní tvorba]

4.7.4.3 Instalace PCNS na doménové řadiče

PCSN je zkratka pro „Password Change Notification Service“, což je služba běžící na doménových řadičích, která umožňuje synchronizovat hesla mezi MIM a AD. Pro její

instalaci bylo připojeno instalační médium pro MIM, stažené v předchozí části, do virtuální mechaniky serveru LG-DC1. Z té byla zkopírována složka „PCNS/x64“ do kořene disku C:. Byl otevřen Powershell a pomocí následujících příkazů byla spuštěna instalace:

```
PS C:\Users\Administrator> cd C:\x64
PS C:\x64> msiexec.exe /i "Password Change Notification Service.msi" SCHEMAONLY=TRUE
PS C:\x64> msiexec.exe /i "Password Change Notification Service.msi"
```

Obrázek 41 - Instalace PCNS [Vlastní tvorba]

Stejný proces byl proveden i na serveru LG-DC2. Následně bylo PCNS nastaveno pomocí následujících příkazů:

```
PS C:\Users\Administrator> cd "C:\Program Files\Microsoft Password Change Notification"
PS C:\Program Files\Microsoft Password Change Notification> setspn -l Administrator
Registered ServicePrincipalNames for CN=Administrator,CN=Users,DC=linet-group,DC=local:
PS C:\Program Files\Microsoft Password Change Notification> setspn -a PCNSCLNT/LG-MIM.linet-group.local LINET-GROUP\admi
Checking domain DC=linet-group,DC=local

Registering ServicePrincipalNames for CN=Administrator,CN=Users,DC=linet-group,DC=local
        PCNSCLNT/LG-MIM.linet-group.local
Updated object
PS C:\Program Files\Microsoft Password Change Notification> .\pcnscfg.exe ADDTARGET /N:LG-MIM /A:LG-MIM.linet-group.local /S:PCNSCLNT/LG-MIM.linet-group.local /FI:"Domain Users"
 /F:1 /I:600 /D:False /WI:60
  Target Name.........: LG-MIM
  Target GUID.........: F8CD135A-4725-4FCD-BBA8-F9946E9D959F
  Server FQDN or Address: LG-MIM.linet-group.local
  Service Principal Name: PCNSCLNT/LG-MIM.linet-group.local
  Authentication Service: Kerberos
  Inclusion Group Name..: LINET-GROUP\Domain Users
  Exclusion Group Name..:
  Keep Alive Interval...: 600 seconds
  User Name Format......: 1
  Queue Warning Level...: 0
  Queue Warning Interval: 60 minutes
  Disabled..............: False
PS C:\Program Files\Microsoft Password Change Notification>
```

Obrázek 42 - Nastavení PCNS [Vlastní tvorba]

4.8 Samoobslužný reset hesla pomocí MIM

Pro nastavení samoobslužného resetu hesla na přihlašovací obrazovce uživatelů je nejprve nutné nastavit synchronizaci mezi AD a MIM

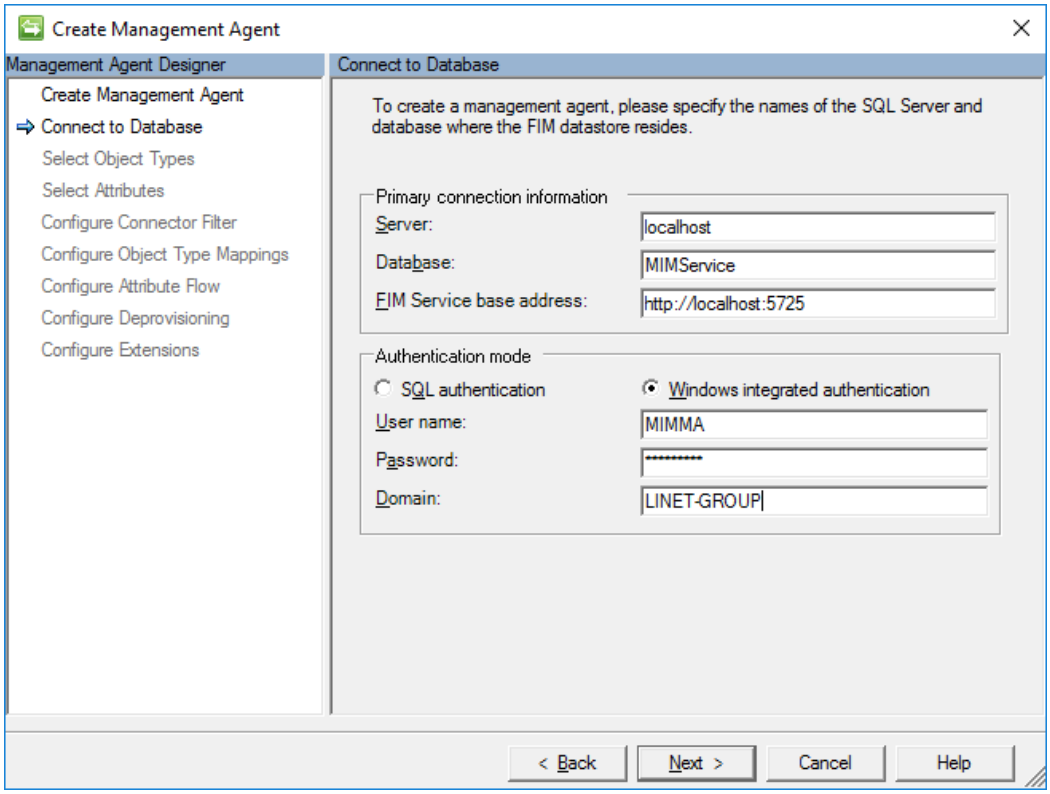
4.8.1 Synchronizace mezi AD a MIM

Na serveru LG-MIM byla otevřena aplikace „Synchronization Service Manager“. V nabídce „Tools“ bylo otevřeno nastavení. Zde bylo povoleno „Enable Synchronization Rule Provisioning“ a „Enable Password Synchronization“.

Poté byla zvolena záložka „Management Agents“, sloužící pro zajištění synchronizace mezi MIM a zdrojem dat (např. AD). Byla zvolena akce „Create“ pro vytvoření nového agenta pro „Active Directory Domain Services“ a agent byl pojmenován LG-DC1. V dalším kroku bylo nutné vyplnit účet, který bude agent využívat pro řízení AD. Pro zvýšení bezpečnosti nebude použit účet „Administrator“, ale dříve vytvořený účet „MIMMA“, kterému bylo přiděleno právnění „Replicating Directory Changes“ pro kořen domény, a umožněno řízení OU „LINET“ a „LINET-GROUP“ s právy pro: „tvorba, mazání a řízení

uživatelských účtů“, „reset uživatelských hesel“, „tvorba, mazání a řízení skupin“ a „úprava členství ve skupinách“. V dalším kroku byla zvolena jediná doména a mezi synchronizované kontejnery byly vybrány ty OU, jejichž řízení bylo přiděleno účtu „MIMMA“, tedy „LINET“ a „LINET-GROUP“. Mezi typy objektů byly přidány uživatelé a skupiny, mezi atributy byly zvoleny: „company“, „department“, „description“, „displayName“, „employeeID“, „employeeType“, „givenName“, „groupType“, „mail“, „member“, „objectSid“, „physicalDeliveryOfficeName“, „postalAddress“, „postalCode“, „sAMAccountName“, „sn“, „st“, „street“, „telephoneNumber“, „title“, „unicodePwd“ a „userAccountControl“. Ostatní kroky tvorby tohoto agenta byly ponechány bez změny.

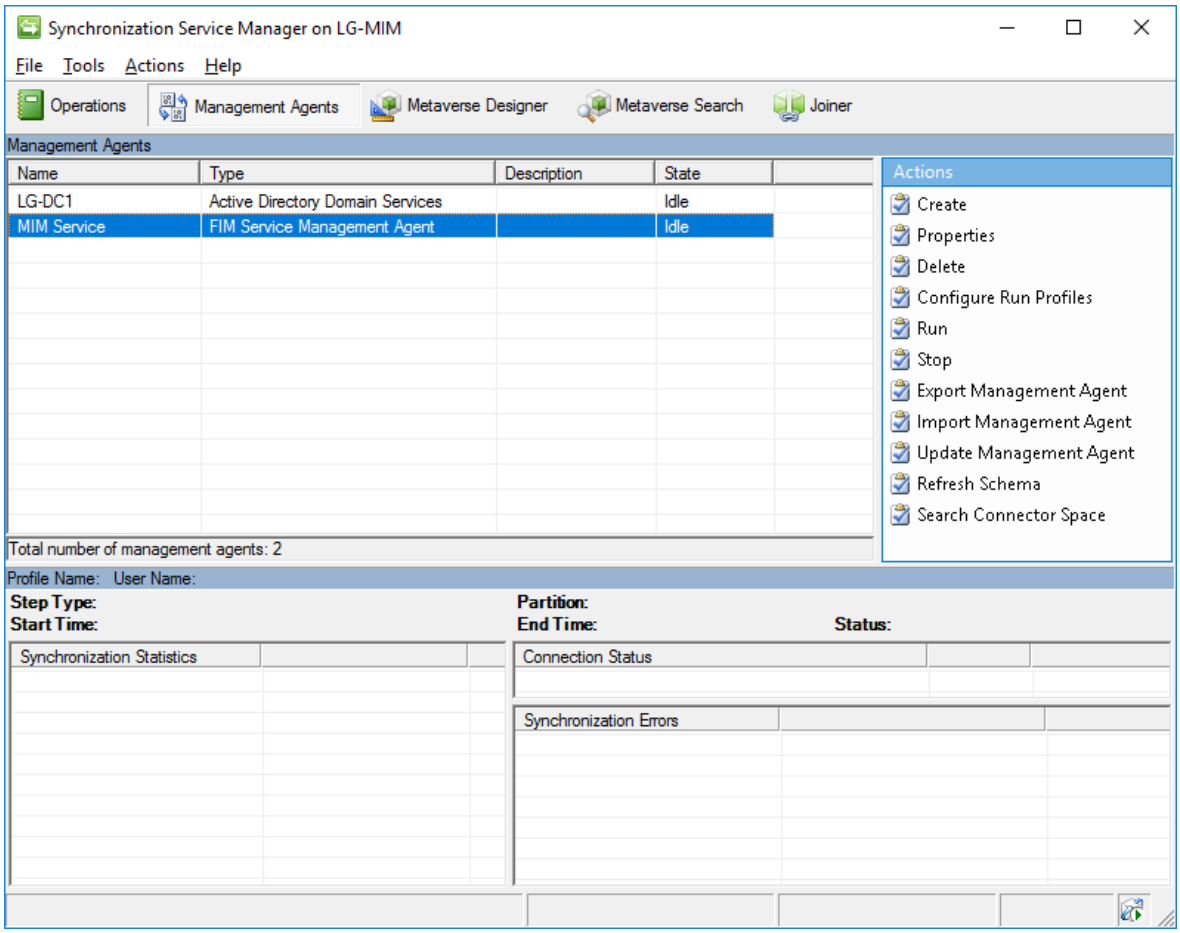
Poté byl vytvořen synchronizační agent pro „FIM Service Management agent“ pojmenovaný „MIM Service“ s vyplněním následujících hodnot:



Obrázek 43 - Tvorba řídícího agenta [Vlastní tvorba]

Před pokračováním byl udělen účtu „MIMMA“ přístup pro zápis do SQL databáze. Poté již mohlo být pokračováno. Později se s přístupovými právy účtu „MIMMA“ vyskytly problémy, proto byl pro účely testování změněn za účet „Administrator“. V následujících dvou krocích byly zvoleny všechny dostupné typy objektů a atributů. Poté bylo přidáno

mapování skupin a osob na výchozí hodnoty. Tok atributů byl přidán dle oficiálního návodu [24]. Ostatní kroky nebyly změněny a agent byl vytvořen.



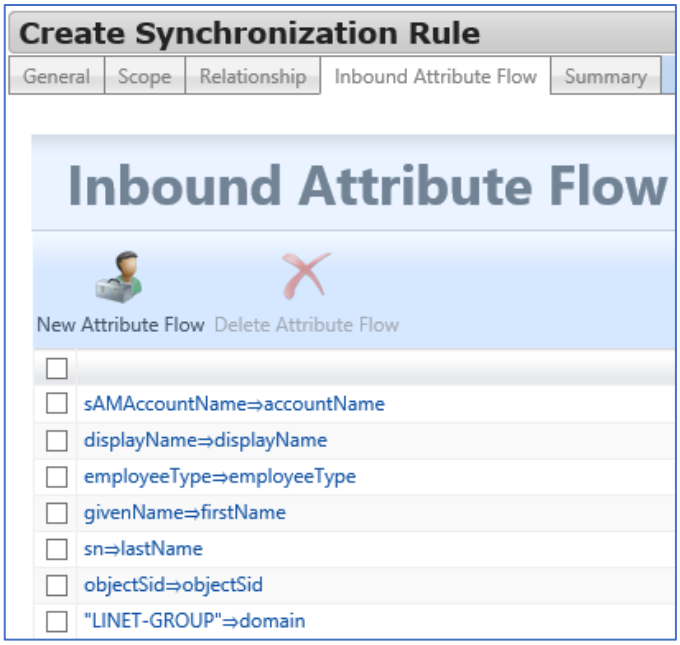
Obrázek 44 - Přehled řídících agentů [Vlastní tvorba]

K oběma agentům byly vytvořeny následující spouštění profily: „Full Import“, „Full Sync“, „Delta Import“, „Delta Sync“ a „Export“ analogicky s příslušným typem. Poté byl spuštěn „Full Import“, kterým se naimportovali 2 uživatelské účty již vytvořené v MIM: „Administrator“ a „Built-in Synchronization Account“. Bylo zkopírování rozlišovací jméno účtu „Administrator“ a bylo přidáno do „Connector Filter“ v nastavení řídícího agenta. Stejný proces byl proveden i pro druhý, synchronizační účet.

4.8.1.1 Tvorba pravidel synchronizace z AD do MIM

Pro synchronizaci AD a MIM je nutné vytvořit pravidla synchronizace. Ve webovém rozhraní MIM bylo zvoleno „Administrator“ – „Synchronization rules“ – „New“. V prvním

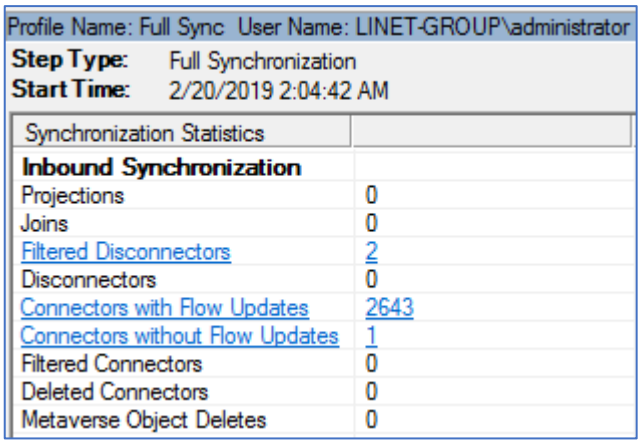
kroku bylo pravidlo pojmenováno „LG-DC1 – Inbound“, v druhém kroku byl zvolen MIM typ „person“, externí systém „LG-DC1“ a externí typ „user“. Ve třetím kroku byl vztah objektů nastaven pomocí atributů „objectSid“ a zvoleno vytvoření zdrojů v FIM (MIM). Poté byly nastaveny toky atributů:



Obrázek 45 - Nastavení toků atributů [Vlastní tvorba]

4.8.1.2 Spuštění synchronizace

Po dokončení tvorby synchronizačního pravidla byl v “Synchronization Service manager” spuštěn opět “Full Import” na agentovi “MIM Service” a tím byl přidán jeden object, kterým bylo právě vytvořené synchronizační pravidlo. Poté byly spuštěny akce “Full Sync”, “Export” a “Delta Import”. Poté byly stejné akce spuštěny na agentovi “LG-DC1”. Na konec byly ještě na agentovi “MIM Service” opět spuštěny akce “Export”, “Full Import” a “Full Sync”, čímž byly naimportovány všechny skupiny a uživatelské účty z AD do MIM, celkem se jedná o 2643 objektů.



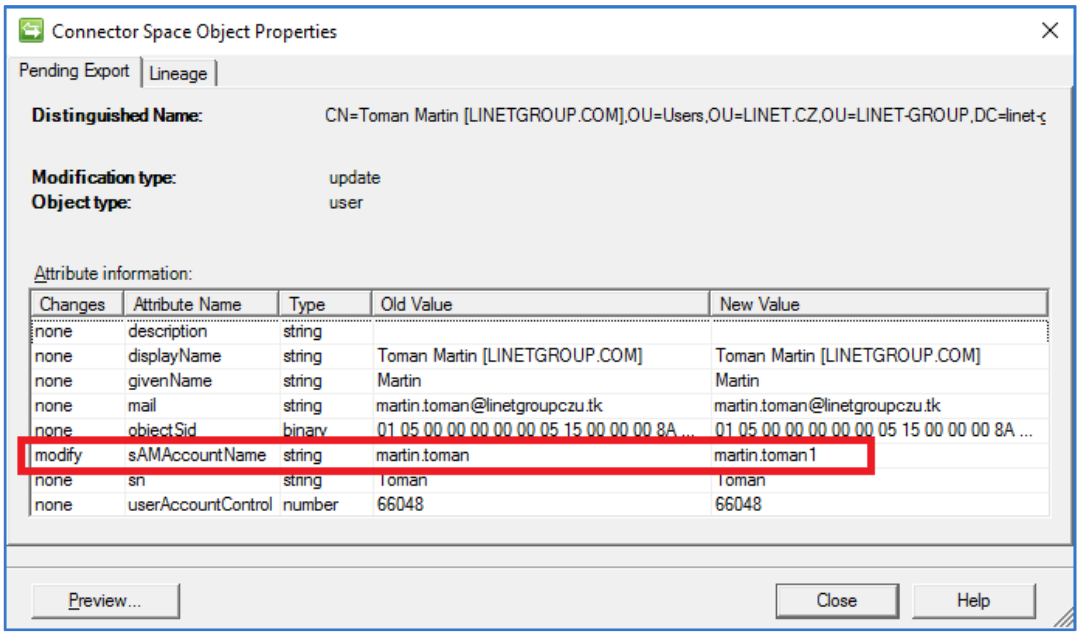
Obrázek 46 - Výsledek synchronizace AD do MIM [Vlastní tvorba]

4.8.1.3 Tvorba pravidel synchronizace z MIM do AD

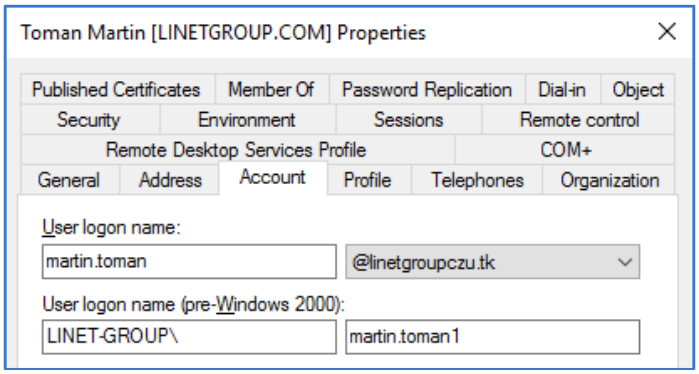
U agenta „MIM Service“ bylo přidáno importování „AccountName“ u položky „Person“ a v nastavení toků atributů bylo ověřeno, že „MIM Service“ má přednost před agentem „LG-DC1“. V portálu MIM v administraci bylo vytvořeno nové synchronizační pravidlo „LG-DC1 – Outbound“, směr toku dat byl změněn na „Outbound“, v dalším kroku byla zvoleny zdroje dat stejně jako při tvorbě „Inbound“ pravidel a „Scoping Filter“ nastaven na „accountName – notEqual – “ tak, aby se synchronizovaly všechny účty, které v „accounName“ obsahují nějakou hodnotu. V nastavení kritérií vztahů byly opět vybrány „objectSid“, v nastavení „Outbound Attribute Flow“ bylo nastaveno: „accountName⇒sAMAccountName“ a průvodce dokončen. V záložce „Metaverse Designer“ bylo u objektu „Person“ zvoleno „Configure Object Deletion Rule“, zvolena dolní možnost „MIM Service“.

4.8.1.4 Testování synchronizace

V portálu MIM bylo u uživatele „LINET-GROUP\martin.toman“ změněno přihlašovací jméno na „LINET-GROUP\martin.toman1“. Poté byly spuštěny akce „Full import“ a „Full Sync“ na agentovi „MIM Service“, a „Full Sync“ a „Export“ na agentovi „LG-DC1“, čímž se upravený účet synchronizoval z MIM do AD.



Obrázek 47 - Synchronizace z MIM do AD [Vlastní tvorba]



Obrázek 48 - Ověření změny přihlašovacího jména v AD [Vlastní tvorba]

4.8.2 Povolení samoobslužného resetu hesla

V portálu MIM bylo otevřeno „Management Policy Rules“ – „Workflow“ a vytvořeno nové pravidlo jménem „_ AD User Provision Workflow“ s typem „Action“. V druhém kroku bylo zvoleno „Synchronization Rule Activity“ a bylo vybráno pravidlo „AD Provisioning Sync Rule“. Poté, kde byly v „Management Policy Rules“ povoleny následující pravidla:

- „Anonymous users can reset their password
- Password reset users set can read password reset objects
- Password Reset Users can update the lockout attribute of themselves
- User management: Users can read attributes of their own

- General: Users can read non-administrative configuration resources
- Administration: Administrators can read and update Users“ [25]

a vytvořeno nové pravidlo: „_ AD User Provisioning MPR“ typu „Request“, žadatelé nastaveny na hodnotu „All People“ a v operacích zvoleny „Create resource“ a „Modify a single-valued attribute“. V dalším kroku byla definována skupina „All Full Time Employees“ a do zdrojového atributu bylo určeno „EmployeeID“. V dalším kroku bylo zvoleno vytvořené workflow: „_ AD User Provision Workflow“.

Další nutnou úpravou bylo povolení účtu MIM Service v WMI na serveru LG-MIM. Byla otevřena konzole „WmiMgmt.msc“ a zvoleno nastavení. Na objekt „ROOT\CIMV2“ byl přidán účet „MIMService“ a byly mu přidány práva „Enable account“, „Remote Enable“ a v rozšířených možnostech byla zvolena platnost i na všechny podobjekty.
Poté bylo v panelu „Component Services“ zvoleno nastavení objektu „My Computer“ a v záložce „COM Security“ byl přidán účet „MIMService“ do všech čtyř možností a byla mu přidělena všechna dostupná práva.

Na serveru LG-MIM byl otevřen IIS Manager a u registrační, i resetovací stránky byl otevřen editor konfigurace, kde byla zvolena sekce: „system.webServer/security/ authentication/windowsAuthentication“ a u „useAppPoolCredentials“ byla zvolena hodnota „True“. Tím bylo umožněno se přihlásit do webových stránek.

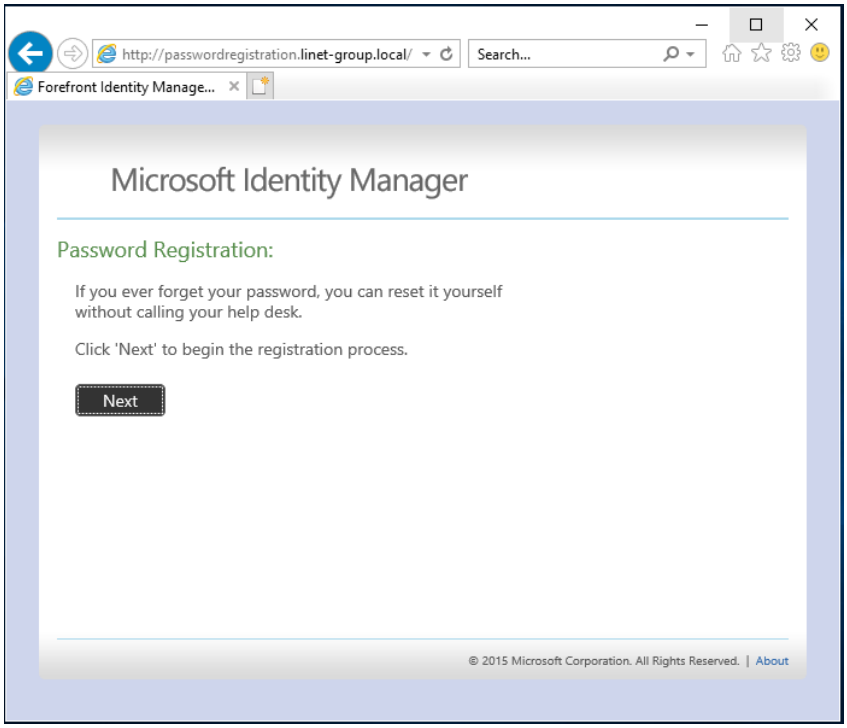
Na serveru „LG-MIM“ byla z virtuálního disku pro instalaci MIM spuštěna instalace „Add-ins and extensions“ – „x64“. Byl vybrán pouze doplněk pro hesla a ověřování, poté byla vyplněna adresa MIM serveru, v dalším kroku webová adresa portálu pro registraci hesla „http://passwordregistration.linet-group.local“ a poté byla spuštěna instalace. Stejný proces byl proveden i na testovacím klientském počítači „CZ1V-1“, kam bylo nutné doinstalovat i doplněk „.NET 3.5“. Poté bylo na serveru „LG-MIM“ v „Synchronization Service Manager“ otevřeno nastavení agenta „LG-DC1“ a v posledním kroku „Configure Extensions“ povoleno: „Enable password management“.

4.8.2.1 **Jazyková úprava dle lokalizace**

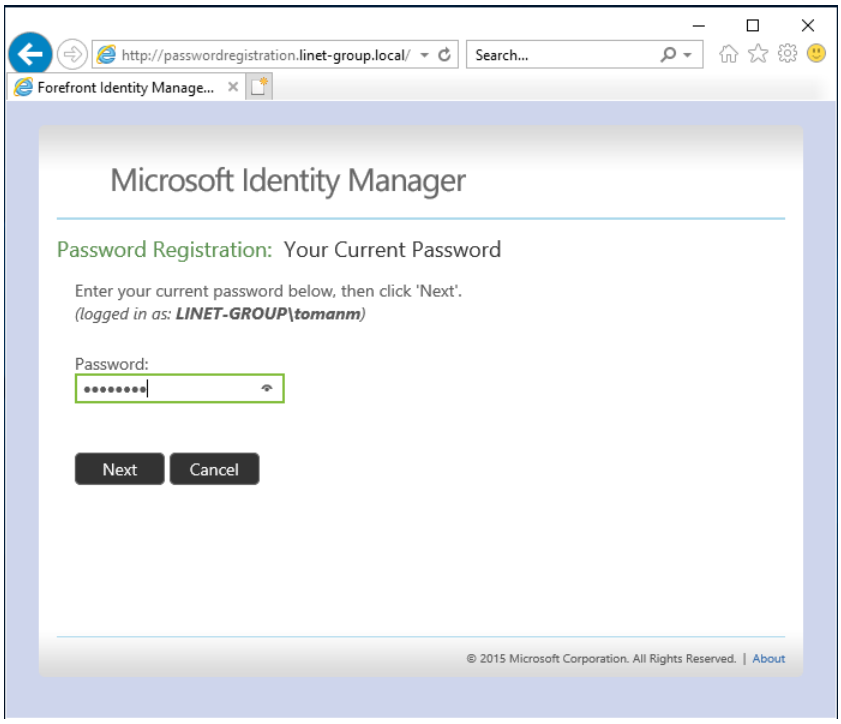
Portál pro registraci a reset hesla je dostupný ve 40 různých jazykových verzích. Použitý jazyk je určen na základě verze instalovaného doplňku, který je jiný pro každý jazyk. Jazykovou mutaci lze tedy určit při instalaci počítače. Testována byla anglická verze.

4.8.3 Testování registrace hesla

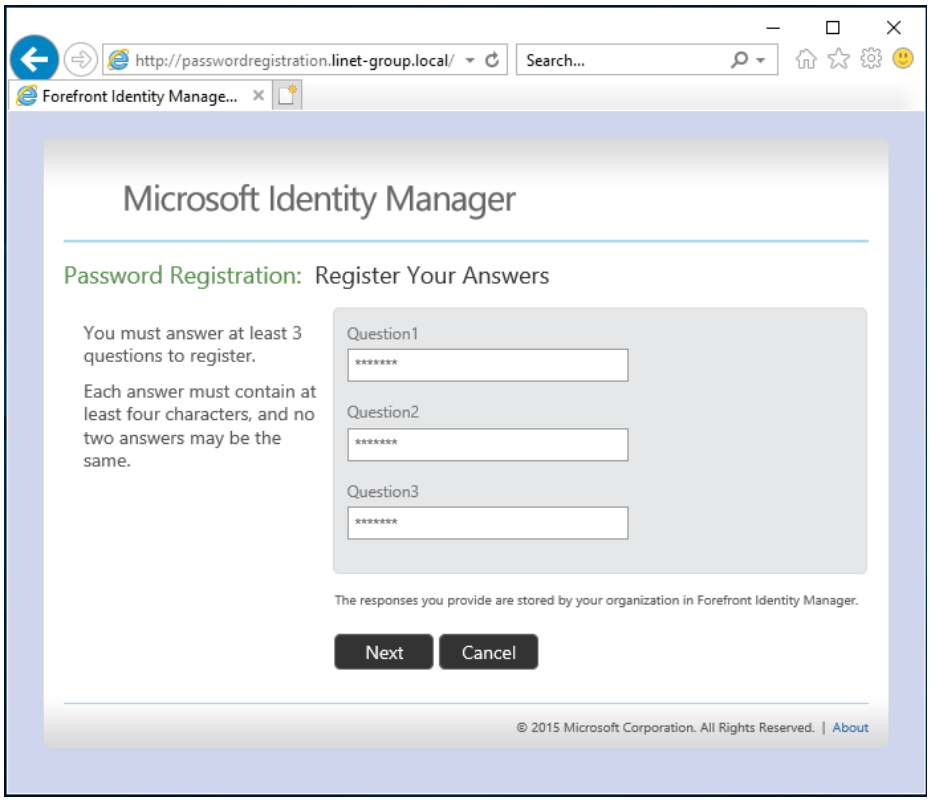
Proces registrace hesla byl otestován na klientské stanici „CZ1V-1“.



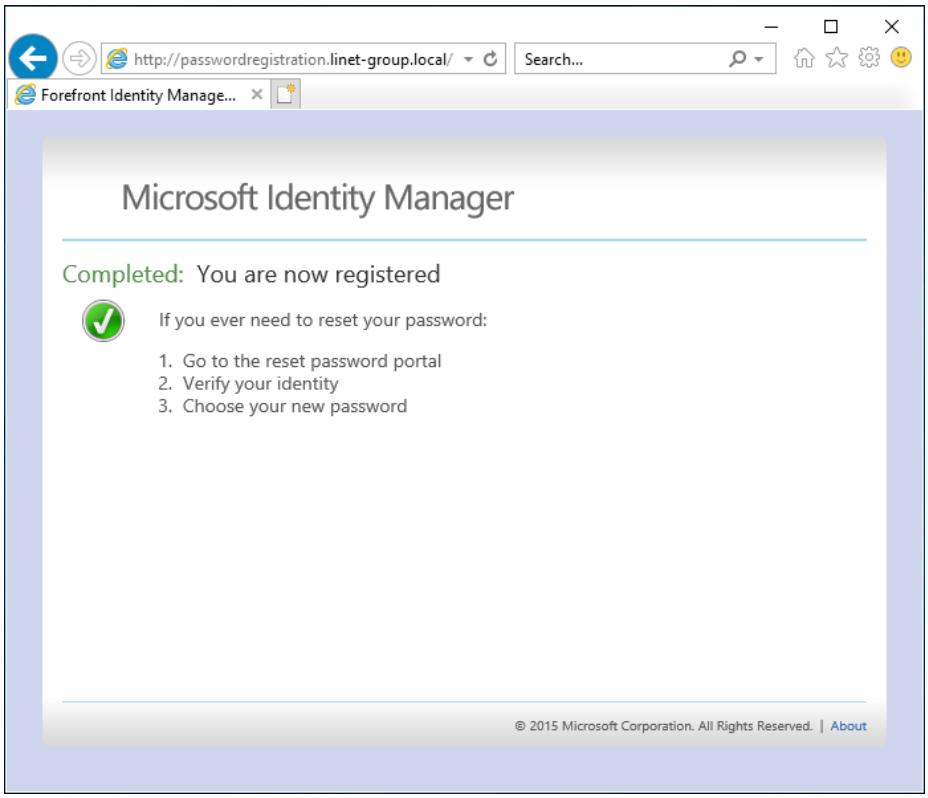
Obrázek 49 - Úvodní obrazovka [Vlastní tvorba]



Obrázek 50 - Vyplnění současného hesla [Vlastní tvorba]

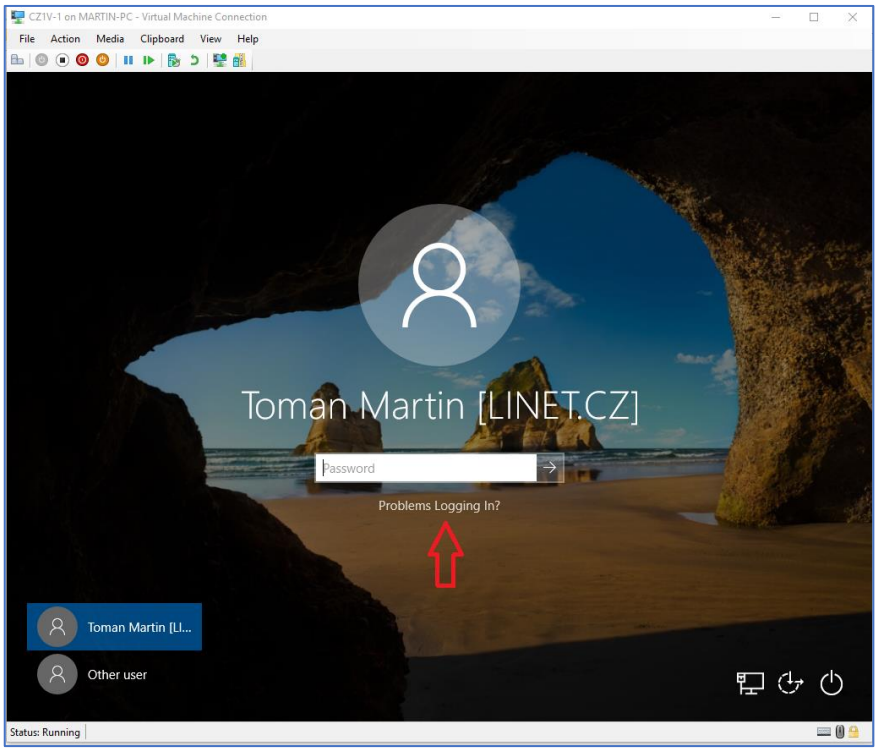


Obrázek 51 - Vyplnění kontrolních odpovědí [Vlastní tvorba]

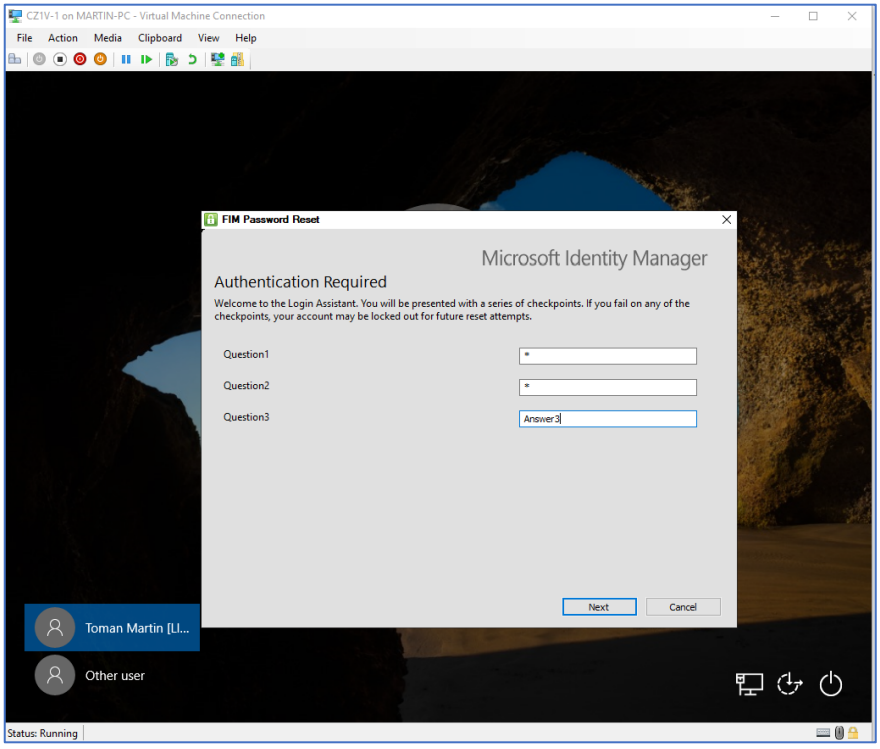


Obrázek 52 - Potvrzení registrace [Vlastní tvorba]

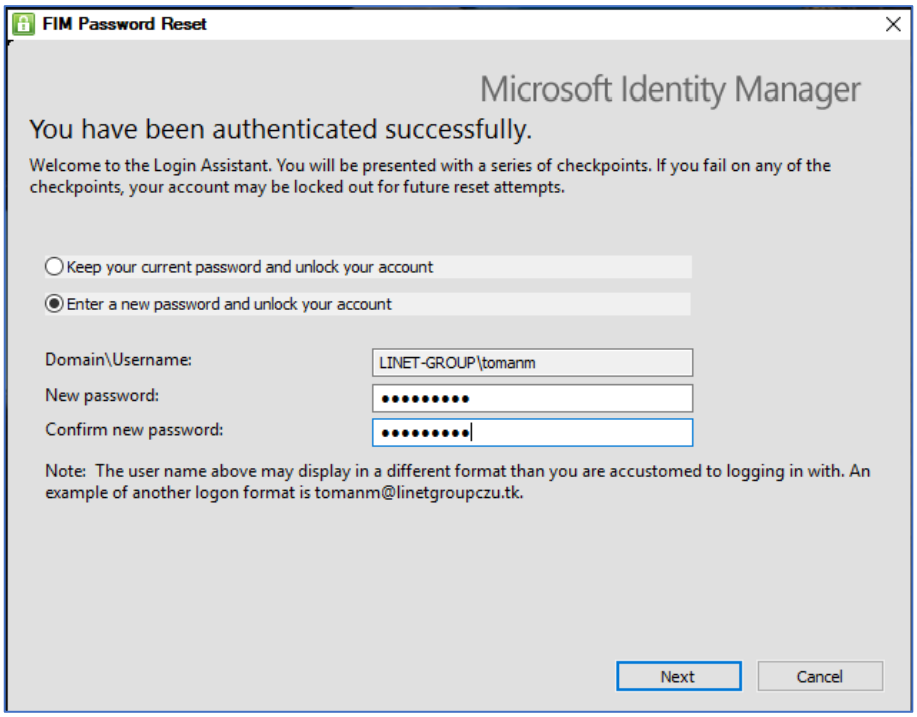
4.8.4 Testování resetu hesla



Obrázek 53 - Odkaz na portál pro reset hesla [Vlastní tvorba]

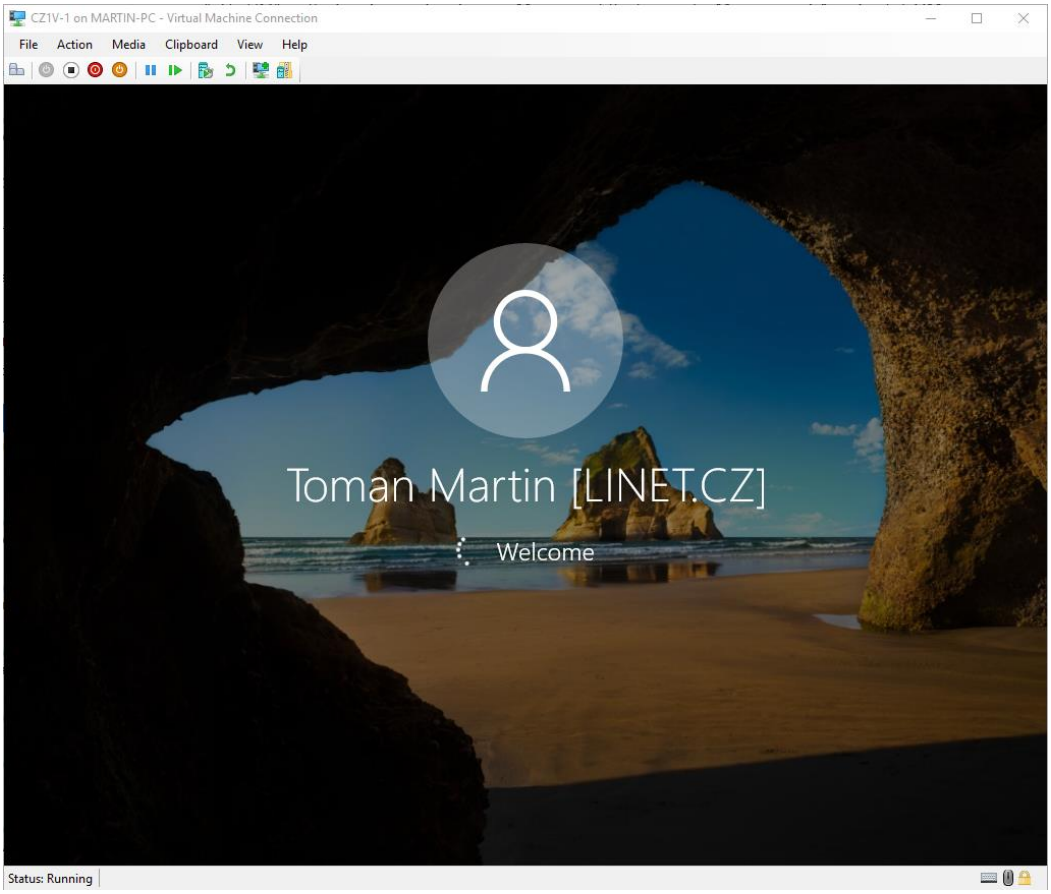


Obrázek 54 - Vyplnění kontrolních odpovědí [Vlastní tvorba]



Obrázek 55 - Vyplnění nového hesla [Vlastní tvorba]

Obrázek 56 - Potvrzení o resetu hesla [Vlastní tvorba]



Obrázek 57 - Přihlášení pomocí nového hesla [Vlastní tvorba]

4.8.5 Výsledek testování

Resetování hesla na přihlašovací obrazovce pomocí zodpovězení kontrolních otázek fungovalo bez problému. Oproti resetu v Azure portálu [Kapitola 4.6] přináší několik výhod: resetování probíhá přímo na počítači uživatele, není potřeba k tomu využít jiné zařízení, které by mohlo odpovědi zkompromitovat, dále neposkytuje uživatelům milnou představu, že mohou resetované heslo použít pro přihlášení do PC i mimo firmu, kde počítač nemůže kontaktovat firemní řadiče pro ověření nového hesla, a je možné jej využít i na stanicích bez přístupu k internetu.

4.9 Návrh na změna řízení účtů – napojení na HR databázi

Řešením na problémy způsobené nedostatečným řízením uživatelských účtů je napojení AD na HR databázi, kde jsou všechny personální změny zanesené. HR databáze je spravovaná pracovníky HR oddělení, jejichž zodpovědnost je udržovat databázi stále aktuální. Pro otestování nastavení napojení HR databáze, AD a MIM byl obnoven záchytný bod serveru LG-MIM do stavu, kdy jsou nainstalované všechny prerekvizity a aplikace MIM, ale nastavená zatím není.

Skutečná HR databáze není veřejně přístupná vzhledem k obsahu, který podléhá ochraně osobních údajů. Proto byla vytvořena testovací HR databáze obsahující 3 testovací uživatele a uložena na server LG-MIM do C:/HRData.txt.

```
EmployeeID:10
DeltaOperation:Add
Company:LINET-GROUP
FirstName:Terry
LastName:Adams
UserID:tadams
EmployeeType:Full Time Employee
Manager:

EmployeeID:11
DeltaOperation:Add
Company:LINET-GROUP
FirstName:Jimmy
LastName:Bischoff
UserID:jbischoff
EmployeeType:Full Time Employee
Manager:10

EmployeeID:12
DeltaOperation:Add
Company:LINET-GROUP
FirstName:Lola
LastName:Jacobsen
UserID:ljacobsen
EmployeeType:Full Time Employee
Manager:11
```

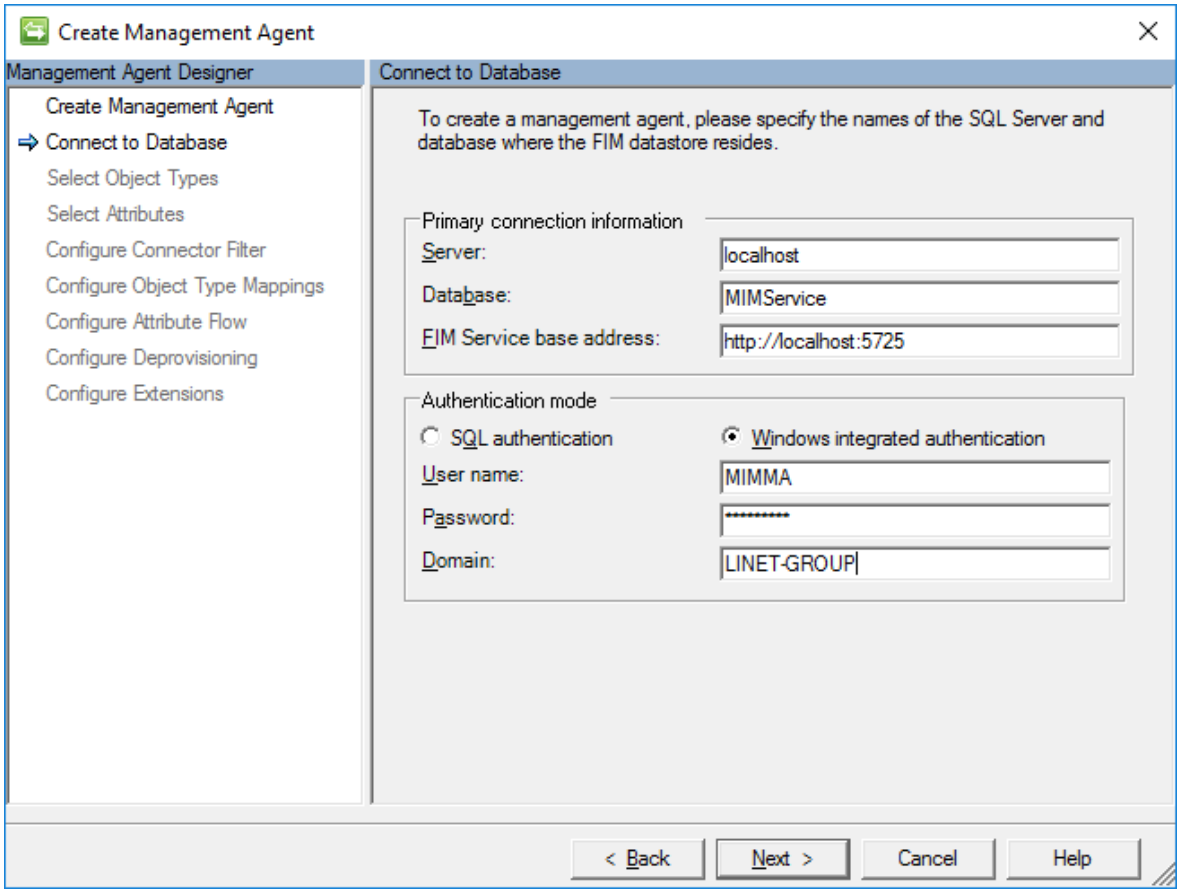
Obrázek 58 - Obsah testovací HR databáze [26]

Poté byla v AD vytvořena organizační jednotka „FIMObject“ s umístěním v „LINET.CZ“ – „Users“, kam budou testovací vytvářené účty ukládány.

Na server LG-MIM byl otevřen nástroj „Synchronization Service Manager“, v záložce „Management Agents“ bylo zvoleno „Create“. Název byl zvolen „HR MA“ a typ

byl vybrán „Attribute-value pair text file“. V druhém kroku byl vybrán textový soubor, který zastupuje HR databázi. Ve třetím kroku v nabídce „Set Anchor“ byl vybrán atribut „EmployeeID“. V nabídce atributů byla zvolena úprava atributu „Manager“ a v typu bylo zvoleno „Reference (DN)“. Ostatní kroky tvorby Management Agenta nebyly měněny.

Poté byl vytvořen synchronizační agent pro „FIM Service Management agent“ pojmenovaný „MIM Service“ s vyplněním následujících hodnot:



Obrázek 59 - Tvorba řídícího agenta [Vlastní tvorba]

V následujících dvou krocích byly zvoleny všechny dostupné typy objektů a atributů. Poté bylo nastaveno mapování skupin a osob na výchozí hodnoty. Tok atributů byl přidán dle oficiálního návodu [26]. Ostatní kroky nebyly změněny a agent byl vytvořen.

Poté byla opět zvolena akce „Create“ pro vytvoření nového agenta pro „Active Directory Domain Services“ a agent byl pojmenován „AD MA“. V dalším kroku bylo nutné vyplnit účet, který bude agent využívat pro řízení AD. Pro zvýšení bezpečnosti nebude použit účet „Administrator“, ale dříve vytvořený účet „MIMMA“, kterému bylo přiděleno

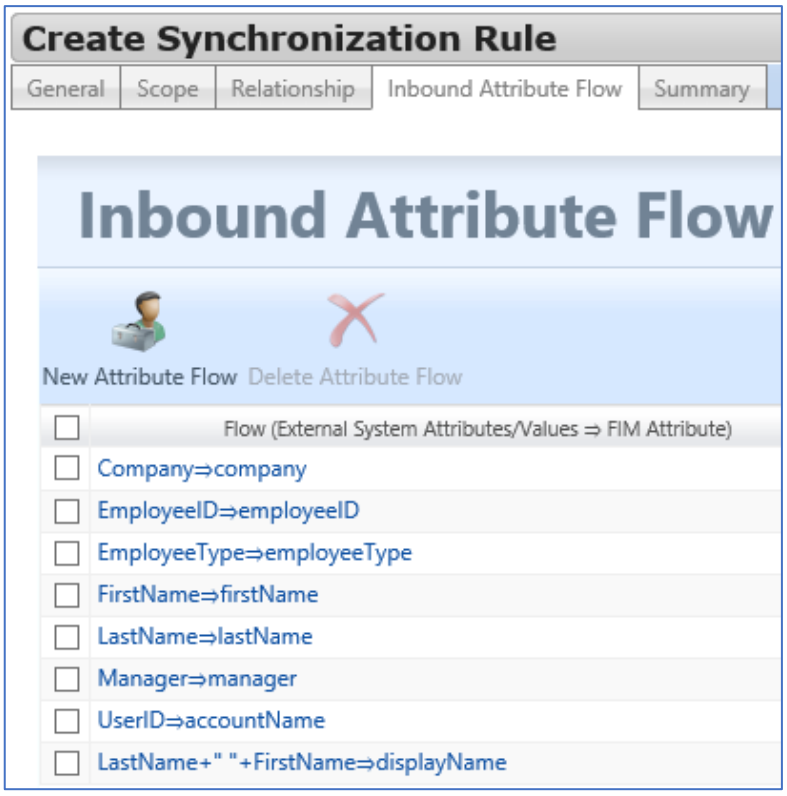
oprávnění „Replicating Directory Changes“ pro kořen domény, a umožněno řízení OU „LINET“ a „LINET-GROUP“ s právy pro: „tvorba, mazání a řízení uživatelských účtů“, „reset uživatelských hesel“, „tvorba, mazání a řízení skupin“ a „úprava členství ve skupinách“. V dalším kroku byla zvolena jediná doména a mezi synchronizované kontejnery bylo vybráno pouze 1 OU pro otestování: „LINET.CZ“. Mezi typy objektů byly přidáni uživatelé, mezi atributy byly zvoleny: „company“, „displayName“, „employeeID“, „employeeType“, „givenName“, „manager“, „objectSid“, „sAMAccountName“, „sn“, „unicodePwd“ a „userAccountControl“. Ostatní kroky tvorby tohoto agenta byly ponechány bez změny. Následně byla testovací HR databáze přesunuta do složky: „C:\Program Files\Microsoft Forefront Identity Manager\2010\Synchronization Service\MaData\HR MA“.

4.9.1 Konfigurace spouštěcích profilů

Pro agenta „HR MA“ byl vytvořen spouštění profil „Full Import“ a do „kolonky vstupní data“ byl přidán soubor s HR databází, a profil „Full Sync“. Pro agenty „AD MA“ i „FIM MA“ byly vytvořeny spouštěcí profily „Full Import“, „Full Sync“, „Delta Import“, „Delta Sync“ a „Export“.

4.9.2 Nastavení synchronizačních pravidel

Bylo nutné vytvořit synchronizační pravidla, která zajistí propojení dat mezi HR databází a MIM, a mezi MIM a AD. Ve webovém rozhraní MIM bylo zvoleno „Administrator“ – „Synchronization rules“ – „New“. V prvním kroku bylo pravidlo pojmenováno „HR User Inbound Synchronization Rule“, v druhém kroku byl zvolen zdrojový typ „person“, externí systém „HR MA“ a externí typ „person“. Ve třetím kroku byl vztah objektů nastaven pomocí atributů „employeeID“ a zvoleno vytvoření zdrojů v FIM (MIM). Poté byly nastaveny toky atributů:



Obrázek 60 - Toky atributů [26]

4.9.3 Nastavení synchronizace z MIM do AD

Nastavení synchronizace se skládá ze čtyř částí: tvorba pravidla synchronizace, vytvoření pracovního postupu, nastavení všech dodavatelů a vytvoření pravidel zásad správy. Pravidlo synchronizace bylo pojmenováno: „AD User Synchronization Rule“, směr toku tak bylo zvolen „Inbound and Outbound“, v druhém kroku byl zvolen MIM typ „person“, externí systém „AD MA“ a externí typ „user“. Ve třetím kroku byl vztah objektů nastaven pomocí atributů „employeeID“ a zvoleno vytvoření zdrojů v Externím systému. Poté byly nastaveny toky Outbound a Inbound atributů dle oficiálních instrukcí od Microsoftu [26].

Vytvoření pracovního postupu je možné v „MIM“ – „MPR“ – „Workflows“ – „New“. Workflow typu „Action“ bylo pojmenováno „AD Provisioning Workflow“. V druhém kroku bylo nastaveno právě vytvořené synchronizační pravidlo „AD User Synchronization Rule“.

Dále byl vytvořen set v „MIM“ – „MPR“ – „Sets“ – „New“, pojmenován „All Contractors and FTEs“, v druhém kroku nastaveni uživatelé, které splňují kterékoliv z následujících podmínek: „Employee Type is Full Time Employee or Contractor“.

Tvorba AD Provisioning MPR byla provedena v „MIM“ – „MPR“ – „New“, jméno zvoleno „AD Provisioning MPR“, typ „Set Transition“. V druhém kroku nastaven set „All Contractors and FTEs“, typ ponechán „Transition In“. Ve třetím kroku zvoleno „AD Provisioning Workflow“. Ostatní kroky nebyly měněny.

Pomocí PowerShellu bylo ověřeno, že jsou pravidla nastaveny správně.:

```
Provisioning Policy Configuration
=================================


SRName    : AD User Synchronization Rule
SRType    : Inbound and Outbound
WFName    : AD Provisioning Workflow
WFAction  : Add
MPRNames  : AD Provisioning MPR

SRName    : HR User Inbound Synchronization Rule
SRType    : Inbound
WFName    :
WFAction  :
MPRNames  :


Command completed successfully
```

Obrázek 61 - Ověření pravidel [Vlastní tvorba]

Inicializace agenta FIM MA proběhla pomocí akcí: „Full Import“, „Full Sync“, „Export“, „Delta Import“. Poté bylo v záložce „Metaverse Designer“ u objektu „person“ nastavena preference HR zdroje u všech synchronizovaných atributů [26]. Poté došlo k inicializaci agenta AD MA spuštěním akcí: „Full Import“ a „Full Sync“.

Pro otestování synchronizace z MIM do AD byly vytvořeny 2 testovací uživatelské účty:

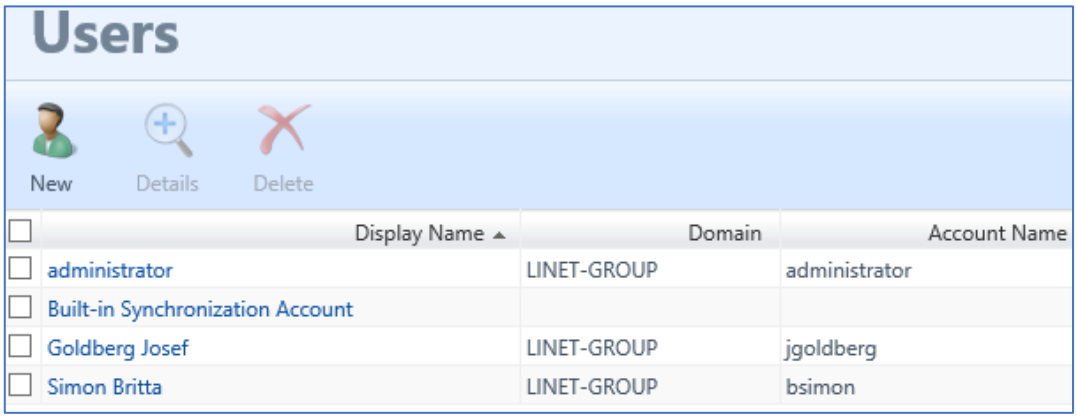
Attribute	User 1	User 2
First Name	Britta	Jossef
Last Name	Simon	Goldbe
Display Name	Britta	Jossef
Account Name	bsimon	jgoldb
Employee Type	Contra	Contra
Employee ID	13	14

Obrázek 62 - Údaje testovacích účtů [Vlastní tvorba]

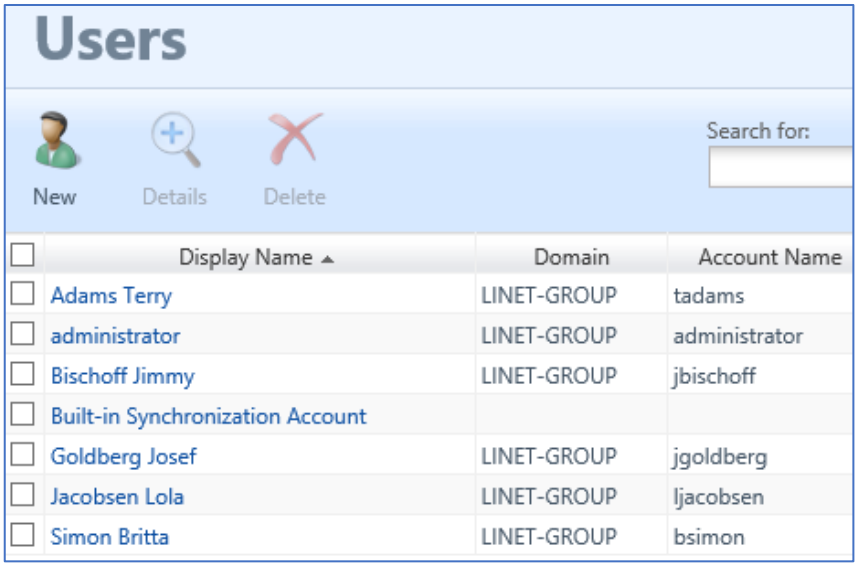
Poté bylo ověřeno, že se oba uživatelé zobrazují v setu „All Contractors and FTEs“ a že mají v záložce „Provisioning“ viditelné pravidlo „AD User Synchronization Rule“, což jsou podmínky pro úspěšnou synchronizaci.

4.9.4 Zpracování HR databáze

Pro přidání HR databáze do MIM byly spuštěny u agenta HR MA akce „Full Import“ a „Full Sync“ a u agenta FIM MA akce „Export“.



Obrázek 63 - Seznam uživatelů před propojením s HR databází [Vlastní tvorba]



Obrázek 64 - Seznam uživatelů po propojení s HR databází [Vlastní tvorba]

Po synchronizaci se uživatelé z HR databáze zobrazili v MIM portálu, v AD ale zatím nejsou.

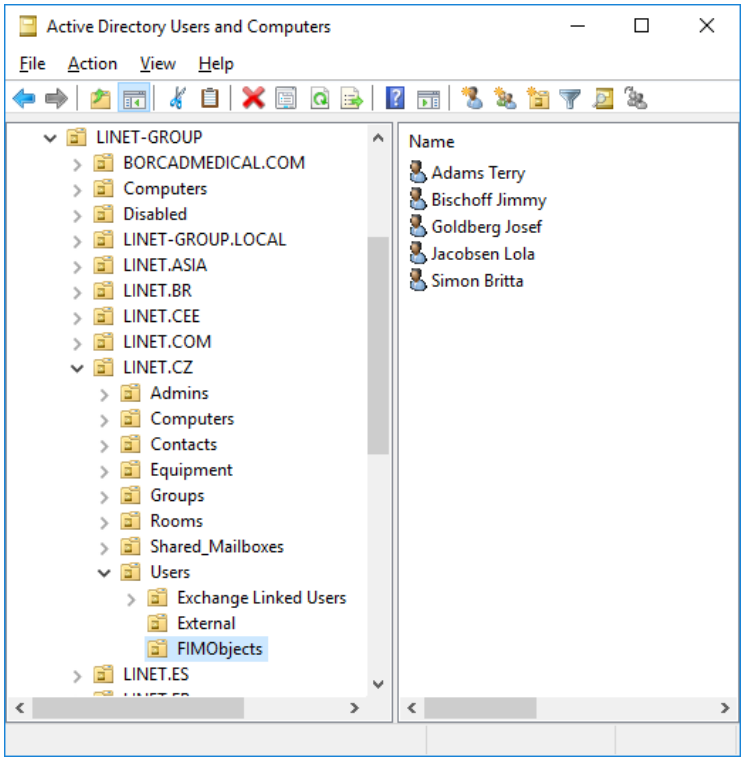
4.9.5 Synchronizace HR databáze do AD prostřednictvím MIM

Pro synchronizaci MIM, který již obsahuje data z HR databáze, do AD, byly spuštěny následující akce „Full Import“ a „Full Sync“ na agentovi FIM MA. Z obrázku je patrné, že se po spuštění exportu v AD vytvoří 5 nových účtů.

Synchronization Statistics	
Inbound Synchronization	
Projections	7
Joins	0
Filtered Disconnectors	2
Disconnectors	0
Connectors with Flow Updates	10
Connectors without Flow Updates	2
Filtered Connectors	0
Deleted Connectors	0
Metaverse Object Deletes	0
Outbound Synchronization	**FIM MA**
Export Attribute Flow	7
Outbound Synchronization	**AD MA**
Export Attribute Flow	5
Provisioning Adds	5

Obrázek 65 - Výsledek akce "Full Sync" na agentovi "FIM MA" [Vlastní tvorba]

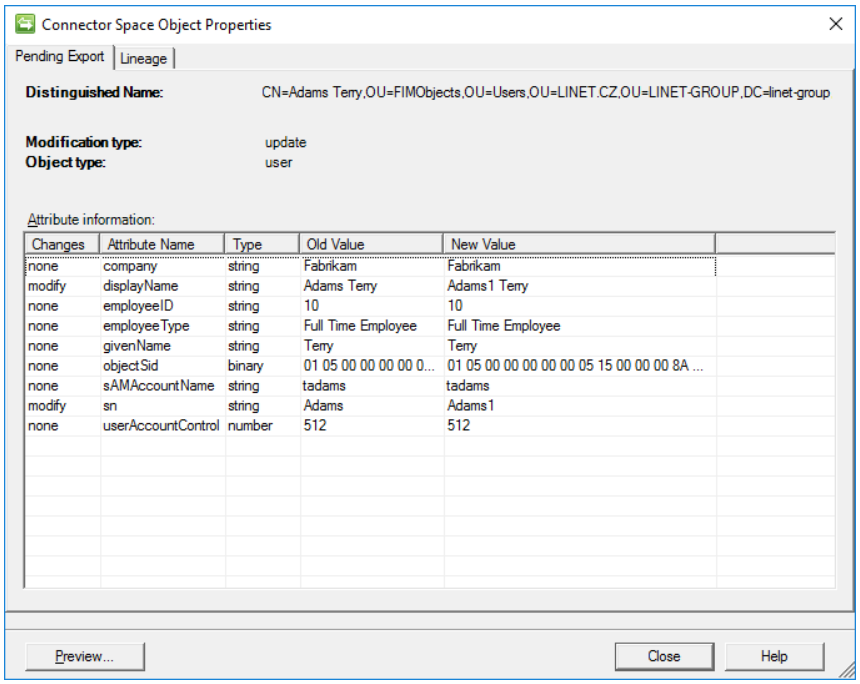
Poté byly spuštěny akce „Export“ a „Full Import“ na agentovi AD MA. Účty byly úspěšně vytvořeny v AD.



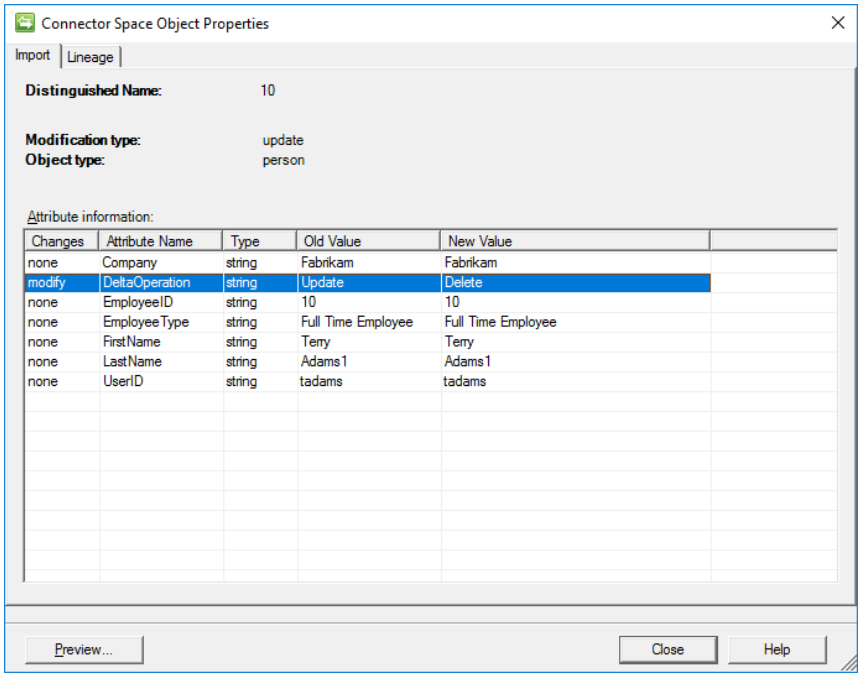
Obrázek 66 - Přehled vytvořených účtů z HR databáze [Vlastní tvorba]

4.9.6 Úpravy a mazání účtů

Pomocí změny obsahu HR databáze u příkazu „DeltaOperation“ z „Add“ na „Update“ nebo „Delete“ je možné snadno měnit záznamy o zaměstnancích, nebo účty mazat.



Obrázek 67 - Změna v AD pomocí změny v HR databázi [Vlastní tvorba]



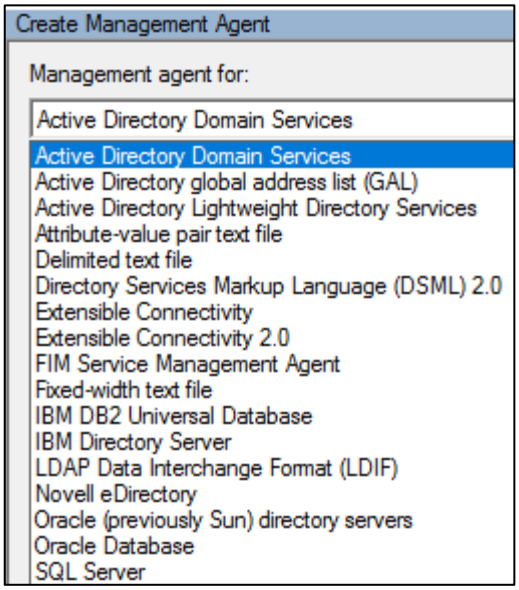
Obrázek 68 - Smazání účtu v AD pomocí změny v HR databázi [Vlastní tvorba]

4.9.7 Výsledek testování

Předpokladem pro napojení je znalost struktury HR databáze, kterou obsluhuje personální systém „OKbase“. Před napojením na HR databázi je nutné v AD definovat jednotlivé pozice zaměstnanců a těm přidělit potřebná oprávnění. Po zadání nového zaměstnance do HR databáze je z MIM zaslána žádost o schválení na budoucího nadřízeného daného zaměstnance a na IT koordinátora. Po schválení je účet automaticky vytvořen se všemi potřebnými oprávněními pro danou pozici.

Při změně pozice je zaměstnanci změněna pozice v HR databázi, MIM zajistí změnu pozice i v AD a tím zaměstnanec přijde o nepotřebná práva a získá potřebná práva. Při odchodu je zaměstnanec zakázán v HR databázi, čímž dojde i k zakázání účtu v AD.

Testována byla pouze synchronizace s AD, ale nástroj MIM umožňuje nastavení synchronizace s velkým množství druhů systémů, které obsahují data o zaměstnancích.



Obrázek 69 - Typy systémů, pro které lze vytvořit řídícího agenta [Vlastní tvorba]

4.10 **Finanční analýza**

Ekonomická analýza je provedena na základě potřebných licencí pro implementaci navrhovaného řešení a výpočtu uspořeného času.

4.10.1 **Náklady**

Náklady se skládají z jednorázových nákladů na implementaci a měsíčních nákladů na licencování. Uvedené částky jsou bez DPH.

- SQL Server Standard licence: 21 055 Kč
- SharePoint Server licence: 113 000 Kč
- Implementace
    - Odhadovaná pracnost: 15 MD.
    - Cena za MD: 8000 Kč.
    - Implementace: 120 000 Kč.
- Microsoft Identity Manager
    - Licence Premium P1 – 135 Kč/uživatel/měsíc
    - 2643 objektů – platí se pouze za uživatele → potřeba 1500 licencí
    - 2 430 000 Kč/rok pro všechny uživatele

4.10.2 **Úspory**

- Reset hesla
    - Průměrná doba celkového zpracování požadavku: 24 minut
    - Odhadovaný počet požadavků měsíčně: 100
    - Ušetřená částka: 10 000 Kč / měsíc (0,4 h*100*250Kč)
- Tvorbou uživatelských účtů
    - Průměrná doba celkového zpracování požadavku: 2 hodiny
    - Odhadovaný počet požadavků měsíčně: 20
    - Ušetřená částka: 10 000 Kč / měsíčně (2 h*20*250Kč)
- Předcházení škodě při zneužití resetovaného hesla, či nezrušeného účtu
    - Pokud by nadále nedocházelo k okamžitému zrušení účtu po odchodu zaměstnance, může dojít ke zneužití nezrušeného účtu, a to může

v extrémním případě vést ke kolapsu celé IT infrastruktury a s tím spojenému kolapsu výroby firmy. Stejný dopad může mít i zjištění hesla uživatele během nezašifrovaného přenosu hesla od IT podpory uživateli.

- Dle plánu obnovy by trvalo úplné obnovení do plného provozu 5 dní.
- Výpadek výroby na 1 den byl vyčíslen na 25 mil. Kč
- Při odhadovaném potenciálním zneužití 1x za 5 let činí úspora 25 mil. ročně.

- Nevyčíslitelné úspory
  - Na vyřešení kritických požadavků, které spadají do SLA1 dle SLA tabulky, má IT podpora 24 hodin. Do úspor je tedy nutné zahrnout jak ušetřenou práci IT pracovníků, tak čas, kdy uživatel čeká na vyřešení. K zapomenutí hesla může dojít v různých situacích a v extrémním případě tím může firma přijít o důležitou zakázku za stovky milionů Kč. Dalším důležitým aspektem je pohodlí uživatelů, které také nelze objektivně vyčíslit.

SLA	Typ požadavku	Čas k řešení	Příklad požadavku
1	Kritický	24 hodin	Nefunkčnosti = nemožno používat IT prostředek nebo systém. Příklad: Nefunkční PC, nefunkční monitor, nefunkční tiskárna, nefunkční IS K2 atd.
2	Závažný	3 dny	Všechny administrativní úkony IT (na základě schválených žádostí). Příklad: Blikající monitor, pomalé PC, nefunkční outlook (je možno pracovat přes webmail), není možno otevřít soubor (ale na jiném PC funguje), vadná baterie v notebooku, založení nového účtu, úpravy adres, atd.
3	Standardní	6 dní	Přidělení IT prostředku, který je skladem, instalace SW atd.
4	Ostatní	15 dní	Pomoc s archivací emailu, nákup IT prostředku atd.
5	Vývojový	45 dní	Nové oko, připojení stroje do kardiogramu atd.

Obrázek 70 - Tabulka SLA [Servicedesk firmy LINET]

4.10.3 **Výsledek**

Náklady na implementaci a provoz systému lze vyčíslit s vysokou přesností, úspory ale mohou být různého charakteru, především zvýšení bezpečnosti času a pohodlí uživatelů, které nelze objektivně vyčíslit. Při započítání potenciálního útoku hackerů 1x za 5 let, který by zastavil výrobu na 5 dní se náklady vrátí již za 1 měsíc.

Náklady	Jednorázové náklady (licence + implementace)	254 055 Kč
	Roční náklady (1500 licencí)	2 430 000 Kč
Úspory	Práce podpory IT (rok)	240 000 Kč
	Předcházení škodě (rok) [Útok 1x/5 let]	25 000 000 Kč
	Nevyčíslitelné úspory (např. pohodlí uživatelů)	

Tabulka 1 - Finanční analýza (částky uvedeny bez DPH)

5 Diskuze

Předmětem práce byla dvě témata: nastavení funkce pro samoobslužný reset hesla a automatizace řízení účtů pomocí propojení AD a HR databáze prostřednictvím MIM. Obě témata vzešly z analýzy současného stavu IT řešení ve firmě Linet.

5.1 Porovnání Azure AD a MIM

Uživatelské prostředí pro registraci i reset hesla v Azure AD má výrazně modernější vzhled a umožňuje více způsobů ověření, oproti prostředí MIM. Na druhou stranu ale využívá webový portál Azure, který je nutné otevřít a přihlásit se do něj. Uživatelé mohou snadno zapomenout adresu portálu. Portál pro registraci hesla v MIM se otevře automaticky po přihlášení do počítače a obnova je možná z přihlašovací obrazovky Windows. Řešení MIM je tedy pro uživatele mnohem dostupnější.

5.2 Zhodnocení automatizace procesů

Způsob implementace propojení HR databáze s MIM a AD není intuitivní a uživatelský přívětivý. Po prvotním správném nastavení již ale procesy probíhají automaticky a do nastavení MIM není potřeba vstupovat. MIM navíc umožňuje napojení na velké množství ostatních systémů, ne pouze AD, jež bylo předmětem testování v této práci.

5.3 Navrhované další kroky

Nejprve je doporučena implementace nástroje MIM a nastavení testovaných funkcí v reálném prostředí firmy. Dalším krokem je implementace nástroje Privileged Access Management (PIM), pro zajištění vyšší bezpečnosti administrátorských účtů. Nástroj přiděluje administrátorům oprávnění podle aktuální potřeby na omezenou dobu. Testování PIM nebylo předmětem této práce.

6 Závěr

Cíle „Usnadnění práce s identitami“ bylo dosaženo napojením AD na HR databázi zaměstnanců pomocí nástroje MIM. Zvýšení uživatelského komfortu bylo dosaženo nastavením funkce na samoobslužný reset v Azure AD a MIM, obě řešení byla porovnána a uživatelsky přívětivější bylo řešení MIM.

V praktické části byla nejprve provedena analýza současného stavu a návrh řešení zjištěných nedostatků pomocí implementace vhodných nástrojů. Poté byla ve virtuálním prostředí nasimulována firemní infrastruktura firmy Linet spol. s r.o. Následně bylo lokální Active Directory propojeno do cloudového Azure Active Directory a nakonfigurována funkce pro samoobslužný reset hesla ve webovém rozhraní. Dále byl do infrastruktury implementován nástroj Microsoft Identity Manager a byly nastaveny funkce pro samoobslužný reset hesla přímo na přihlašovací obrazovce klientského počítače. Poté byla vytvořena testovací HR databáze, ta byla pomocí nástroje MIM propojena do AD a nastaveny funkce pro automatickou tvorbu uživatelských účtů po zadání zaměstnance do HR databáze. Uvedená řešení byla otestována a zhodnocena.

Náklady byly vyčísleny na 254 055 Kč bez DPH jednorázově za implementaci, a poté 2 430 000 Kč bez DPH ročně za licence. Některé úspory nebylo možné objektivně vyčíslit, proto není možné určit návratnost této investice. Přínosy implementace jsou ale znatelné (např. zvýšení bezpečnosti, uživatelského komfortu, …), proto bylo firmě důrazně doporučeno nástroj implementovat.

Následujícím krokem, po dokončení navrhované implementace, je konfigurace nástroje „Privileged Access Management“, který je již součástí nástroje MIM, pro zajištění vyššího zabezpečení administrátorských účtů.

7 Seznam použitých zdrojů

[1] BEYNON-DAVIES, Paul. *DATABASE SYSTEMS*. 3. New York: Palgrave Macmillan, 2004. ISBN 978-1-4039-1601-3.

[2] *SystemOnLine: Principy řízení identit* [online]. Brno: CCB, spol. s r. o., 2012 [cit. 2018-11-09]. Dostupné z: https://www.systemonline.cz/it-security/principy-rizeni-identit.htm

[3] *Identita* [online]. Plzeň: Management Mania, 2015 [cit. 2018-11-25]. Dostupné z: https://managementmania.com/cs/identita

[4] *CO JE TO IDENTITY MANAGEMENT?* [online]. Praha: Computerworld, 2015 [cit. 2018-10-16]. Dostupné z: https://www.ami.cz/publikujeme/blog/co-je-to-identity-management-serial-o-idm-cast-1

[5] *Hlavní oblasti ITSM dle ITIL®* [online]. Praha: O2 IT Service s.r.o., 2016 [cit. 2018-10-22]. Dostupné z: http://www.itil.cz/index.php?id=989

[6] RUEST, Danielle a Nelson RUEST. *Virtualizace: podrobný průvodce*. . Brno: Computer Press, 2010. ISBN 978-80-251-2676-9.

[7] TOMAN, Martin. *Zlepšování služeb pro koncové uživatele pomocí System Center*. Praha, 2016. BP. Česká Zemědělská Univerzita v Praze. Vedoucí práce Ing. Martin Havránek, Ph.D.

[8] *PowerShell 6: Začínáme s Windows PowerShellem* [online]. Redmond: Microsoft, 2017 [cit. 2018-10-16]. Dostupné z: https://docs.microsoft.com/cs-cz/powershell/scripting/getting-started/getting-started-with-windows-powershell?view=powershell-6

[9] *W3Techs: Usage of web servers for websites* [online]. Enzersdorf: W3Techs, 2019 [cit. 2019-02-27]. Dostupné z: https://w3techs.com/technologies/overview/web_server/all

[10] STANEK, William R. *Active Directory: kapesní rádce administrátora*. . Brno: Computer Press, 2009. Microsoft (Computer Press). ISBN 978-80-251-2555-7.

[11] *Azure Active Directory: Bezproblémová a zabezpečená správa identit a přístupu* [online]. Redmont: Microsoft, 2018 [cit. 2018-10-16]. Dostupné z: https://azure.microsoft.com/cs-cz/services/active-directory/

[12] *Microsoft Azure: Azure AD directory roles you can manage in PIM* [online]. Redmont: Microsoft, 2018 [cit. 2018-11-09]. Dostupné z: https://docs.microsoft.com/cs-cz/azure/active-directory/privileged-identity-management/pim-roles

[13] *Dokumentace k Microsoft Identity Manageru* [online]. Redmont: Microsoft, 2016 [cit. 2018-10-16]. Dostupné z: https://docs.microsoft.com/cs-cz/microsoft-identity-manager/

[14] CANNER, Ben. Identity Management: Buyer's Guide. *Solution Review: Comparing the Top Identity and Access Management Solutions* [online]. 2018, **2018**(1), 41 [cit. 2018-11-09]. Dostupné z: https://solutionsreview.com/identity-management/get-a-free-identity-and-access-management-software-solutions-buyers-guide/

[15] *Salesforce* [online]. London: Salesforce.com, inc., 2018 [cit. 2018-11-29]. Dostupné z: https://www.salesforce.com

[16] *LINET: O nás* [online]. Slaný: Linet, 2015 [cit. 2019-02-10]. Dostupné z: http://www.linet.com/cs/o-nas

[17] *Microsoft DreamSpark* [online]. Redmont: Microsoft, 2018 [cit. 2019-01-13]. Dostupné z: https://dreamspark.czu.cz/

[18] *Microsoft Download Center: Microsoft Azure Active Directory Connect* [online]. Redmont: Microsoft, 2018 [cit. 2019-02-22]. Dostupné z: https://www.microsoft.com/en-us/download/details.aspx?id=47594

[19] *Microsoft Docs: Nastavení domény* [online]. Redmont: Microsoft, 2018 [cit. 2019-02-14]. Dostupné z: https://docs.microsoft.com/cs-cz/microsoft-identity-manager/preparing-domain

[20] *Microsoft Docs: Nastavení serveru správy identit: Windows Server 2016* [online]. Redmont: Microsoft, 2018 [cit. 2019-02-13]. Dostupné z: https://docs.microsoft.com/cs-cz/microsoft-identity-manager/prepare-server-ws2016

[21] *Microsoft Docs: Nastavení serveru správy identit: SQL Server 2016* [online]. Redmont: Microsoft, 2018 [cit. 2019-02-27]. Dostupné z: https://docs.microsoft.com/cs-cz/microsoft-identity-manager/prepare-server-sql2016

[22] *Microsoft SQL Docs: Download SQL Server Management Studio (SSMS)* [online]. Redmont: Microsoft, 2018 [cit. 2019-02-15]. Dostupné z: https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-2017

[23] *Microsoft Evaluation Center: Microsoft Identity Manager 2016 SP1* [online]. Redmont: Microsoft, 2016 [cit. 2019-02-15]. Dostupné z: https://www.microsoft.com/en-us/evalcenter/evaluate-microsoft-identity-manager-2016

[24] *Microsoft Docs: Install MIM 2016: Synchronize Active Directory and MIM Service* [online]. Redmont: Microsoft, 2017 [cit. 2019-02-20]. Dostupné z: https://docs.microsoft.com/en-us/microsoft-identity-manager/install-mim-sync-ad-service

[25] *Microsoft Docs: Configure Self-Service Password Reset* [online]. Redmont: Microsoft, 2012 [cit. 2019-02-20]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/mim/hh824694%28v%3dws.10%29

[26] *Microsoft Docs: Introduction to Publishing To Active Directory from Two Authoritative Data Sources* [online]. Redmont: Microsoft, 2012 [cit. 2019-02-22]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/mim/ee534908(v%3dws.10)

8 Seznam příloh

Přílohy

Příloha I - Výstupní list

LINET

VÝSTUPNÍ LIST

JMÉNO A PŘÍJMENÍ VYSTUPUJÍCÍHO PRACOVNÍKA:		DATUM POČÁTKU PRACOVNÍHO POMĚRU: DATUM UKONČENÍ PRACOVNÍHO POMĚRU:
POTVRZENÍ O VYROVNÁNÍ ZÁVAZKŮ		
NÁZEV ODDĚLENÍ	ZÁVAZEK	PODPIS ODPOVĚDNÉHO PRACOVNÍKA POTVRZUJE VYROVNÁNÍ ZÁVAZKU VYSTUPUJÍCÍHO PRACOVNÍKA SE SPOLEČNOSTÍ LINET SPOL. S R.O. JMÉNO, DATUM A PODPIS *POZNÁMKY
POKLADNA	ZÁLOHY VYROVNÁNY ANO □□□□□ □NE □	POKLADNÍ
KVALITA	MĚŘIDLA VYROVNÁNA ANO □□□□□ □NE □	VEDOUCÍ KONTROLY KVALITY
PERSONÁLNÍ ODDĚLENÍ	DOKUMENTACE A OSVĚDČENÍ VYROVNÁNY ANO □□□□□ □NE □	HR SPECIALISTA
PERSONÁLNÍ ODDĚLENÍ	BENEFITY VYROVNÁNY ANO □□□□□ □NE □	RECEPČNÍ
OBCHOD	ZÁPŮJČKY VYROVNÁNY ANO □□□□□ □NE □	BACK OFFICE MANAGER
IT	PŘÍSTUP DO IS OŠETŘEN ANO □□□□□ □NE □	VEDOUCÍ IT
VÝROBA	PRACOVNÍ ODĚVY VYROVNÁNY ANO □□□□□ □NE □	MZDOVÁ ÚČETNÍ
SPRÁVA MAJETKU A ÚDRŽBA	EVIDOVANÝ MAJETEK, KLÍČE VYROVNÁNY ANO □□□□□ □NE □	VEDOUCÍ ÚDRŽBY
INVENTURNÍ MAJETEK	EVIDENCE INVENTURNÍHO MAJETKU ANO □□□□□ □NE □	FINANČNÍ ÚČETNÍ
MZDOVÁ ÚČTÁRNA	ČIPOVÁ KARTA VRÁCENA ANO □□□□□ □NE □	MZDOVÁ ÚČETNÍ
MZDOVÁ ÚČTÁRNA	PODKLADY K UKONČENÍ PP ANO □□□□□ □NE □	MZDOVÁ ÚČETNÍ
MZDOVÁ ÚČTÁRNA	PŘEDÁNÍ ŽÁDANKY O VÝSTUPNÍ LÉKAŘSKOU PROHLÍDKU	PŘEVZAL VYSTUPUJÍCÍ PRACOVNÍK
• NEDOKONČENÁ PRÁCE A DOKUMENTACE PŘEDÁNA NÁSTUPCI (VČ. DOKUMENTU PŘEDÁNÍ PRACOVNÍCH AKTIVIT) • PRACOVIŠTĚ PŘEDÁNO.		PŘÍMÝ NADŘÍZENÝ PODPIS VYSTUPUJÍCÍHO PRACOVNÍKA:
PRACOVNÍK UKONČEN		MZDOVÁ ÚČETNÍ:

Příloha II - IT formulář "Odchod zaměstnance"

ODCHOD ZAMĚSTNANCE

Jméno:		Příjmení:	
Osobní číslo:		Pozice:	

Činnost	Provedeno	Datum	Podpis
HESLO UŽIVATELE – změna na administrátorské	1st support		
Automatická odpověď na Exchange (ECP)	1st Support		
Smazání složky H:/OSOBNÍ/jmeno odchoziho	1st support		
K2 – deaktivace účtu	Michal T. / Michaela L.		
AM – převzetí IT majetku (nebo přepsání na nástupce, nadřízeného)	2nd Support		
-	-	-	-
VÝSTUPNÍ FORMULÁŘ - podepsání (pokud jsou provedeny všechny výše uvedené úkoly)	It manager-zástupce		
-	-	-	-
SALESFORCE – převedení dat na nástupce	Jakub P.		
SALESFORCE – odebrání licence	Jakub P.		
SAP B1 – deaktivace účtu a odebrání licence	Jakub P.		
PRESENTIGO – odebrání účtu	Jakub P.		
AIRWATCH – odebrání licence	Martin T		
LICENCE Office 365 – odebrání	Mira S.		
Adobe Creative cloud	Petr N.		
SERVICEDESK - převedení požadavků na jiného uživatele	1st Support		
KOPÍRKY CANON – smazání	1st Support		
TELEFONNÍ ÚSTŘEDNA – smazání linky (nebo přepsaní na nástupce)	1st Support		
TELEFONNÍ SEZNAM (Intranet) - smazání kontaktu	1st Support		
LYNC – smazat účet	1st Support		
LINET.LOCAL – disable účtu přesunout do OU pro vyřazené a napsat DATUM kdy se tak stalo	1st Support		
LINET-GROUP.LOCAL - disable účtu přesunout do OU pro vyřazené a napsat DATUM kdy se tak stalo	1st Support		

Za IT provedl:
Datum:
Podpis: