Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedtra informačního inženýrství

Bakalářská práce

Integrace počítačů Mac do firemní sítě

Martin Fučík

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Fučík

Systémové inženýrství a informatika
Informatika

Název práce

Integrace počítačů Mac do firemní sítě

Název anglicky

Integrate Macs into your corporate network

Cíle práce

Cílem práce je ukázat, že je možné provozovat platformu Mac ve firemní síti založené na Active Directory (Windows server) včetně využíváni uživatelských profilů v Active Directory.
Vedlejší cíle jsou:
- charakterizace potřeb běžné firemní sítě
- ukázka softwaru třetích stran, který doplňuje chybějící funkce ze strany Windows server nebo řeší nedostatky na straně macOS
- představení open directory od firmy Apple a její nevýhody

Metodika

Metodika řešení problematiky bakalářské práce je založena na studii dokumentace Windows server, macOS a další odborné literatury či internetových zdrojů.

- definujte nedostatky při přímé integraci macOS do Active Directory s možnostmi jejich řešení.

- prakticky demonstrujte způsob nasazení v reálných situacích a nastavení počítačů Mac.

- formulujte závěry a doporučení.

Doporučený rozsah práce

30-40

Klíčová slova

Windows server, Active Directory, Open Direcrtory, Mac, Firemní síť, MDM

Doporučené zdroje informací

Pavlicek J., Pavlickova P., Naplava P., Measures of quality in Business Process Modeling, EOMAS 2019

Předběžný termín obhajoby

2021/22 ZS – PEF

Vedoucí práce

Ing. Josef Pavlíček, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 19. 11. 2020

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 11. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 25. 11. 2021

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Integrace počítačů Mac do firemní sítě" jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské 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(ka) uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30.11.2021 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Josefu Pavlíčkovi, PhD. za vedení a podporu této práce. Zároveň bych rád poděkoval spolupracovníkům a klientům společnosti logiconal s.r.o. za možnost pracovat s jejich počítačovými sítěmi.

Integrace počítačů Mac do firemní sítě

Abstrakt

V bakalářské práci se věnuji tématu integrace počítačů Mac do firemní počítačové sítě, která je založená na Active Directory. Požadavek na integraci počítačů Mac mají administrátoři počítačových sítí čím dál častěji a v případě, kdy Macy tvoří minoritu, tak k němu administrátoři přistupují jako k dalšímu počítači s Windows. Mac je na tento postup sice připraven, ale jen možností integrace do Active Directory, který uživateli umožní se přihlásit svými údaji k Macu a načíst svojí domovskou složku. Následně už není žádná příprava, která by umožňovala napojení na již existující bezpečností politiky. To následně bývá „trnem v oku“ administrátorů, kteří problém řeší komplikovaně nebo ho neřeší vůbec. Cílem práce je zhodnotit postup přímého napojení do Active Directory, ukázat software třetích stran, který odstraňuje nedostatky Windows server nebo macOS. V praktické části práce je provedeno šetření, které poukazuje na nespolehlivost přímé integrace do Active Directory. Následně je popsáno praktické nasazení softwaru třetích stran pro eliminaci nedostatků. Závěrem jsou formulovány doporučení pro Integraci počítače Mac do firemní sítě.

Klíčová slova: Windows server, Active Directory, Open Directory, Mac, Firemní síť, MDM

Integrate Macs into your corporate network

Abstract

This thesis examines the topic of integration of Mac computers into a corporate computer network based on Active Directory. The requirement for Mac integration is more and more frequently being requested among administrators of computer networks, and when Macs are a minority, administrators treat them as just another Windows computer. The Mac is ready for this, but only by integrating with Active Directory, which allows the user to log in with their Mac credentials and retrieve their home folder. Further, there is no preparation that allows for connection to pre-existing security policies. This subsequently tends to be a "thorn in the side" of administrators who solve the problem in a complicated manner or not at all. The aim of this paper is to evaluate the process of direct linking to Active Directory, to show third party software that complements the shortcomings of Windows server or macOS. In the practical part of the thesis, an investigation is carried out that points out the unreliability of direct integration into Active Directory. Subsequently, the practical deployment of third-party software to eliminate the shortcomings is described. Finally, recommendations are formulated for Mac integration into the corporate network.

Keywords: Mac, Windows server, Active Directory, Open Directory, Corporate network, MDM

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AD	Active Directory
OD	Open Directory
DS	Directory service . adresářová služba
MDM	Mobile Device Management
LDAP	Lightweight Directory Access Protocol
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
XML	Extensible Markup Language
MECM	Microsoft Endpoint Configuration Manager

1 Úvod

Firemní počítačové sítě jsou už několik let základem pro práci v každé větší firmě. Řeší autentizaci uživatelů, pracovních stanic, sdílení dat, bezpečnostní politiky a mnoho dalších funkcí, které konkrétní firma může vyžadovat. Díky úspěchu společnosti Microsoft se svým operačním systémem Windows je většina těchto sítí založena na serverové edici tohoto operačního systému. V průběhu posledních 15 let stoupla popularita počítačů Mac od společnosti Apple natolik, že se začali u správců počítačových sítí objevovat požadavky na integraci počítačů Mac do sítě, která je založená právě na Windows server.

K vybrání tohoto tématu mě vedla práce ve společnosti zabývající se servisem počítačů Mac a následné založení vlastní společnosti, která se mimo jiné zabývá i jejich integrací do firemních sítí. Během integračních procesů u malých a středních podniků, které v minulosti investovali nemalé prostředky do platformy Windows jsem zjistil, že Mac je sice připraven pro fungování v prostředí Active Directory, ale v reálném provozu nasazení do Active Directory „pokulhává“.

Při přímé integraci Maca do Active Directory řeší správce počítačové sítě obvykle problémy s přihlášením uživatele, distribuce a aktualizace softwaru nebo nastavení bezpečnostních politik, které jsou řešeny jinak, než je to v případě systému Windows v Active Directory. Na řešení těchto problémů většinou neexistuje postup v oficiální dokumentaci, která například možné problémy s přihlášením uživatele ani nezmiňuje. Většina literatury, která se těmito problémy zabývá je z důvodu rychlého vývoje macOS již neaktuální. Správci sítě Active Directory, tak povětšinou nedisponují uceleným postupem, který by mohli použít.

Obsahem této práce je popsání přímé integrace počítačů Mac do Active Directory, definování nedostatků a možnostmi jejich řešení, které je realizováno pomocí softwaru třetích stran. Software je vybrán, tak aby co nejlépe eliminoval nedostatky.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je ukázat, že je možné provozovat platformu Mac ve firemní síti založené na Active Direcotry (Windows server) včetně využívání uživatelských profilů v Active Directory.

Vedlejší cíle jsou

- Charakterizace potřeb běžné firemní sítě.
- Ukázka softwaru třetích stran, který doplňuje chybějící funkce ze strany Windows server nebo řeší nedostatky na straně macOS.
- Představení Open Directory od firmy Apple a její nevýhody.

2.2 Metodika

Metodika řešení problematiky bakalářské práce je založena na studii dokumentace Windows server, macOS a další odborné literatury či internetových zdrojů.

- Definujte nedostatky při přímé integraci macOS do Active Directory s možnostmi jejich řešení.
- Prakticky demonstrujte způsob nasazení v reálných situacích a nastavení počítačů Mac.
- Formulujte závěry a doporučení.

3 Teoretická východiska

3.1 Firemní síť

Firemní síť (anglicky Enterprise network nebo Corporate network) je pojem, který označuje komunikační páteř pro zajištění přenosu dat napříč odděleními, pracovními skupinami a lidmi. Klíčovým účelem firemní sítě je zabránit izolaci některých uživatelů či skupin. Všechny zařízení a systémy, které se v síti nachází by měli být schopny komunikovat mezi sebou. Kromě toho by fyzické i softwarové systémy měli být schopny poskytovat uspokojivý výkon, spolehlivost a bezpečnost. Rozsah a požadavky firemní sítě můžou být velmi odlišné podle provozních a resortních požadavcích.

Obvyklým účelem sítě je pak integrovat všechny systémy, včetně počítačů a operačních systémů Windows a macOS, unixových systémů, mainframů a dalších souvisejících zařízení jako jsou tablety, telefony nebo tiskárny. Úzce integrovaná firemní síť pak kombinuje a využívá různé komunikační protokoly, zařízení a systémy. [4]

Struktura, která pokrývá běžné potřeby takovéto sítě se skládá ze zařízení, které komunikují uvnitř sítě, tak i poskytuji internetové připojení do vně sítě. Typická infrastruktura firemní sítě se skládá z:

- Síťového hardwaru
- Síťového softwaru
- Síťových služeb

Mezi síťový hardware patří prvky jako router, switch, síťová karta, přístupový bod nebo kabeláž. V softwarové části najdeme operační systémy, aplikace na správu sítě a bezpečnostní aplikace. V části služeb pak najde různé druhy připojení k internetu a síťové protokoly. Jednotlivé prvky, které se v síti nachází se škálují podle potřeb konkrétní sítě a organizace. [2][5]

Pro zajištění komunikace mezi pracovními stanicemi, operačními systémy, uživateli a pracovními skupinami je potřeba nasadit software, který vytvoří prostředí zajišťující tyto

požadavky. Tento software bývá součástí distribuce serverových edicí operačních systémů. Pro rozsáhlost popularity operačního systému Windows se tak obvykle volí operační systém Windows server.

Serverová editace operačního systému dokáže zajistit prakticky všechny požadavky na software a služby, které neumí zajistit ostatní síťové prvky. Běžná firemní počítačová síť potřebuje pro svůj provoz na serveru provozovat alespoň tyto služby [2]:

- Adresářové služby
- Domain Name System (DNS server)
- Dynamic Host Configuration Protocol (DHCP server)

3.1.1 Adresářové služby

Adresářová služba (DS) je aplikace či skupina aplikací, které dokážou zajišťovat komunikaci mezi stanicemi, uživateli a skupinami uvnitř počítačové sítě. Funguje také jako centrální autentizační autorita.

Adresářová služba využívá pro komunikaci Lightweight Directory Access Protocol (LDAP), což je aplikační rozhraní pro dotazování a modifikaci adresářových služeb nad protokolem TCP/IP. LDAP lze popsat pomocí čtyř modelů:

- Informační model
- Jmenný model
- Funkční model
- Bezpečností model

Více informací o DS a LDAP zde [6]

3.1.1.1 Active Directory

Active Directory (AD) je adresářová služba od společnosti Microsoft, která je součástí Windows Server. Služba v sobě ukrývá rozsáhlé schopnosti pro správu firemní počítačové sítě. AD pracuje s objekty jako jsou servery, stanice, aplikace, uživatelé a uživatelské skupiny. Tyto objekty lze třídit mezi organizační jednotky, což je jakýsi kontejner do, kterého jsou objekty vkládány. Uživatelé musí být schopni tyto informace nalézt a použít.

Dále v sobě AD zahrnuje řadu služeb, které poskytují autentizaci, autorizaci (pro autorizaci a autentizaci je využívám protokol LADP a bezpečnostní protokol Kerberos) a správu uživatelů. Jiné funkce pak usnadňují správu objektů v AD. Mezi ně patří Group Policy, které určují, co je a co není povoleno na určitých stanicích nebo pro určité uživatele.

Základním prvkem logické struktury je doména. Do té jsou přímo uloženy objekty, které patří do domény. Z těchto důvodů je celá služba velmi úzce napojena na DNS server, který by měl ideálně běžet na serveru, z kterého je služba AD poskytována.

Nasazení AD ve firemní síti pro koncového uživatele znamená možnost sdílet data s ostatními uživateli v AD, ale také možnost přihlásit se svým účtem na libovolné stanici v AD. [2][7]

3.1.1.2 Open Directory

Open Directory (OD) je adresářová služba od společnosti Apple, která je součástí aplikace Server pro macOS. Je vytvořená pomocí několika open source aplikací a ve své podstatě funguje podobně jako AD, kdy základní logickou strukturou je doména. Autentizace a autorizace probíhá také za pomocí protokolů LDAP a Kerberos. Klienti OD mají podobně jako u AD přístup ke svým uživatelským účtům, datům atd.

Historicky byla OD používáná v sítích, kde byli pouze počítače Mac nebo v kombinaci s AD. Kombinace AD a OD je podle Applu oficiálně nazývá Dual Diracotry, ale běžně je toto řešení známé spíš jako „Zlatý trojúhelník“ nebo „Magický trojúhelník“, protože se sním řešili nedostatky přímé integrace macOS do AD.

V dnešní době je sice OD stále k dispozici v aplikaci Server, nicméně už není dál rozvíjena. Vzhledem k tomu, že Apple postupně odstraňuje funkce z aplikace Server, tak není úplně vhodné použít OD k řešení nedostatků přímě integrace do AD. Navíc je možné, že Apple brzo ukončí podporu, a tak nemá moc smysl na OD stavět firemní síť.

Náhradou za „Zlatý trojúhelník“ je dnes využívání služby MDM. Například Apple Profile Manager, který je součástí aplikace Server. [1]

3.2 Mac v prostředí AD

Počítač Mac jde připojit k AD pomocí konektoru (pluginu) pro AD, který je v macOS. Připojit se lze k AD, která je na serveru provozovaná na Windows Server 2008 a novější (v případě, že se aktivuje „slabé šifrování“, tak se lze připojit i k Windows Server 2000 a novější). Konektor pro AD generuje veškeré atributy, které jsou nutné pro ověření totožnosti v systému macOS v rámci uživatelských účtů AD. Dále je podporována změna hesla uživatele, získání časových údajů o vypršení hesla a získání základních údajů o uživatelském účtu.

Pro zjištění topologie domény využívá macOS DNS. K ověření totožnosti je využíván protokol Kerberos a k identifikaci uživatelů a skupin protokol LDAP verze 3. Dále je možné nastavit připojení obrazu disků nebo domovské složky pomocí protokolu SMB.

Pro mobilní počítače Mac je možné při integraci do AD nastavit „mobilní účet“. Při prvním přihlášení uživatele dojde k vytvoření lokálního účtu v Macu, který bude nadále synchronizován s AD. To umožňuje využívání uživatelského účtu z AD i v momentě, kdy Mac není připojen k síti, kde nachází AD. [8][9][11]

3.3 Mobile Device Management na Macu

Mobile Device Management (MDM) je způsob, jak bezpečnou a bezdrátovou formou konfigurovat zařízení, které jsou v majetku organizace nebo uživatele. Službou MDM můžeme nastavovat a monitorovat dodržování pravidel organizace nebo mazání a zamykání zařízení na dálku.

Mac se do MDM registruje pomocí registračního profilu, což je konfigurační profil, který zařízení registruje u MDM. Jakmile je zařízení registrováno, tak je možné distribuovat ostatní konfigurační profily, kterými můžeme zařízení spravovat. [13] [14]

3.3.1 Konfigurační profil

Konfigurační profil je XML soubor s příponou .mobileconfig. Konfigurační profily umožňují automaticky konfigurovat nastavení, účty, omezení a pověřovací údaje. Jediné, co nejde pomocí konfiguračního profilu měnit je uživatelské jméno a heslo. Konfigurační profily lze vytvářet ve službě MDM, v aplikaci pro vytváření konfiguračních profilů nebo je lze vytvořit ručně.

Konfigurační profily lze šifrovat a podepisovat. Tím jde omezit jich použití na konkrétních zařízení Apple a zároveň zabránit případnému zneužití. [13] [14]

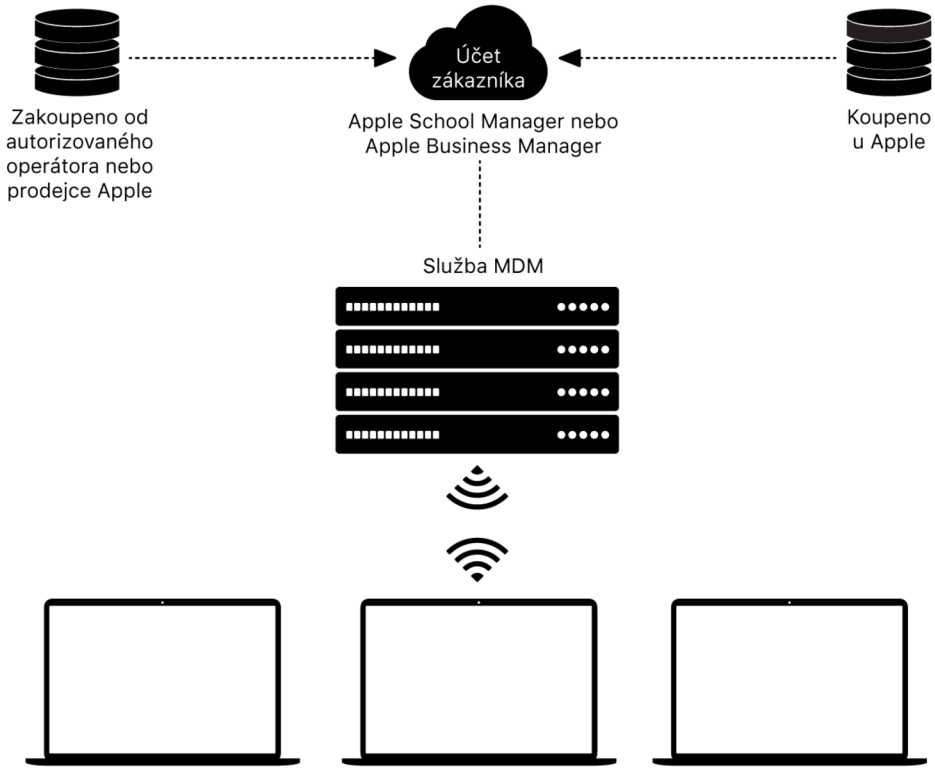
3.3.2 Služby MDM

Pro využívání služby MDM můžeme využít Apple Profile Manager, který je součástí Serverové aplikace pro macOS. Můžeme také zvolit jakoukoliv jinou službu MDM.

Pro vybrání vhodné služby MDM vychází každý rok několik srovnání, které nám mohou usnadnit výběr. [25]

3.3.3 Služby Applu pro hromadnou správu zařízení

K MDM lze připojit služby Apple Business Manager nebo Apple School Manager, které umožnují automaticky distribuovat registrační profil a následně další konfigurační profily na nová zařízení, která jsou ve vlastnictví organizace. [13] [14]



Obrázek 1 - Vizualizace MDM a služeb pro hromadnou správu zařízení, zdroj: [28]

3.4 Software třetích stran

3.4.1 NoMAD

NoMAD je open source aplikace, která umožňuje Macu využívat funkce AD, které nabízí AD plugin v macOS bez nutnosti přímé integrace. Uživatelé na Macu využívají lokální účty, které na Macu již existují a jednoduše spustí aplikaci NoMAD. Po spuštění se aplikace podívá, jestli je Mac připojen k AD. Pokud není, je uživatel vyzván k zadání domény AD. Následně aplikace využije DNS k vyhledání AD.

V případě, že je Mac přímo integrován do AD a NoMAD dokáže přečíst informace o připojení, tak se uživatel může přihlásit svým AD účtem. Po úspěšném přihlášení NoMAD načte pomocí Kerberos záznamy o uživateli. Následně zobrazí jméno, spočítá exspiraci hesla, najde domovskou složku uživatele či načte jiné záznamy. Pokud uživateli exspiruje heslo NoMAD umožní jeho změnu a propíše změnu do AD. [15][16]

3.4.2 NoMAD Login

NoMAD Login je open source aplikace, která nabízí nahrazení přihlašovacího okna macOS za okno, které umí komunikovat s AD. Přímá integraci opět není potřeba. Uživatel během přihlášení zadá své uživatelské jméno ve tvaru *jmeno@domena*. Pokud je doména dostupná NoMAD Login se připojí k AD a na základě údajů uživatele vytvoří totožný lokální účet. Přihlašovací okno NoMAD Login také umožňuje přihlášení k jakýmkoliv již existujícím lokálním účtům.

Aplikace disponuje mnoha dalšími funkcemi, včetně těchto:

- Demobilizace mobilního účtu AD
- Podpora šifrování disku pomocí FileVault
- Úprava UI přihlašovacího okna

Pro synchronizaci lokálního účtu vytvořený pomocí NoMAD Login s AD directory lze použít aplikaci NoMAD. [17]

Další podrobnosti o nastavení aplikace lze nalézt [18]

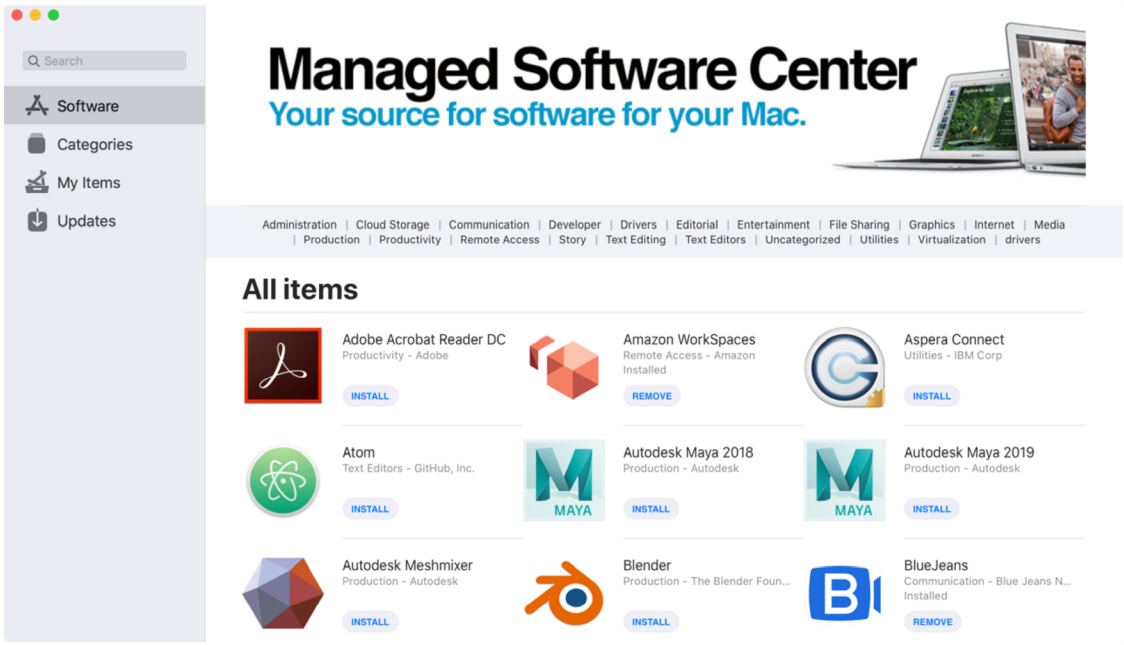
3.4.3 Munki

Munki je open source aplikace vyvinutá společností Walt Disney Animation Studios. Jedná se o sadu nástrojů, které společně tvoří webový repositář s daty. To umožňuje administrátorům Macu spravovat instalace (v mnoha případě i odinstalován) softwaru v macOS. Kromě povinných instalací, které se automaticky instalují na každou stanici, Munki disponuje i možnostmi pro volitelný software, kde si mohou uživatelé stahovat aplikace podle vlastního uvážení. Munki lze také nastavit pro distribuci systémových aktualizací macOS.

Pro koncového uživatele je součástí Munki aplikace Managed Software Center, kde uživatel vidí aktualizace aplikací nebo systému. Dále si zde může stahovat volitelné aplikace podle svého uvážení. [19]

Celý nástroj je v podstatě jednoduchý web server, který se skládá ze tří částí:

- Instalační soubory
- Katalogy
- Manifesty



Obrázek 2 - Ukázka aplikace Managed Software Cenrer, zdroj: [27]

3.4.3.1 Instalační soubory

Zde se nachází diskové obrazy anebo softwarové balíčky. Ve většině případů stačí použít ty, které vývojář softwaru běžně poskytuje. [21]

3.4.3.2 Katalogy

Katalogy představují seznam dostupného softwaru a obsahují meta data o instalátorech softwaru. [21]

3.4.3.3 Manifesty

Manifest obsahuje informace softwaru z přiřazených katalogů. Určíme v něm, který software by měl být nainstalován nebo odinstalován na konkrétních stanicích a také dobrovolný software pro koncového uživatele. Každá stanice může mít vlastní manifest nebo můžeme mít jeden pro více stanic. [21]

3.4.4 MunkiAdmin

Jedná se o jednoduchou aplikaci pro macOS, která umožňuje spravovat Katalogy a Manifesty pro aplikaci Munki pomocí grafického rozhraní. Umožňuje tak lepší přehled o aktuálních katalogách a snadnější vytváření a správu Manifestů. [22]

3.4.5 AutoPkg

Jedná se o framework pro macOS, který automatizuje vytváření a distribuci softwarových balíčků. Tyto činnosti, které se jinak dělají manuálně, jsou tak zautomatizovány. AutoPkg plně připraví software pro hromadnou distribuci na spravované stanice. [23]

3.4.5.1 AutoPkgr

Jedná se o open source aplikaci, které umožní instalaci a správu AutoPkg pomocí GUI. Dále zajistí snadné stahovaní softwaru, sledování aktualizací, notifikace pro administrátory, snadný přístup do adresářů používaných frameworkem AutoPkg a snadnou integraci s Munki či dalšími aplikacemi pro správu softwaru. [24]

3.4.6 Parallels Device Management

V sítích AD, které využívají Mictosoft Endpoint Configuration Manager (MECM) lze použít plugin Parallels Device Management, který rozšíří možnosti MECM o snadnější správu počítačů Mac nebo iOS zařízení. [26]

4 Vlastní práce

Integrace počítačů Mac byla testována a prováděná na firemních počítačových sítích, kde byl provozován Windows Server 2016 s aktivní službu AD, do které bylo přidáno mezi 20-45 počítači s Windows 10. Počítače Mac, které byli použity k testování a zisku veškerých daty obsahovali operační systém macOS 11 Big Sur. Pro zvláštní testování upgradu na macOS 11 Big Sur byl použit macOS 10.15 Catalina. Cílem praktické části je ukázat možnosti reálného nasazení počítačů Mac v prostředí, které spoléhá na AD. Počítače Mac vždy v těchto sítích tvořili minoritní zastoupení v řádu jednotek kusů.

4.1 Přímá integrace do AD

Přímá integrace do AD je možná třemi způsoby. Pokaždé je využíván plugin pro AD, který se nachází v macOS. V ideálním případě by Mac, který má být takto integrován do AD měl být po čisté instalaci macOS, tedy smazání disku a instalace aktuální verze macOS (či požadované verze), ale vyžadováno to není.

Před integrací je potřeba vytvořit na Macu účet správce, který bude fungovat jako lokální administrátor. Lze ho pojmenovat třeba „LocalAdmin“. Pod tímto účtem by měl administrátor provádět veškeré nastavení potřebné pro integraci s AD. Po integraci je při určitém nastavení možné použít administrátorské účty z AD. V tomto případě slouží lokální administrátor pouze jako pojistka v případě přerušení spojení Maca s AD.

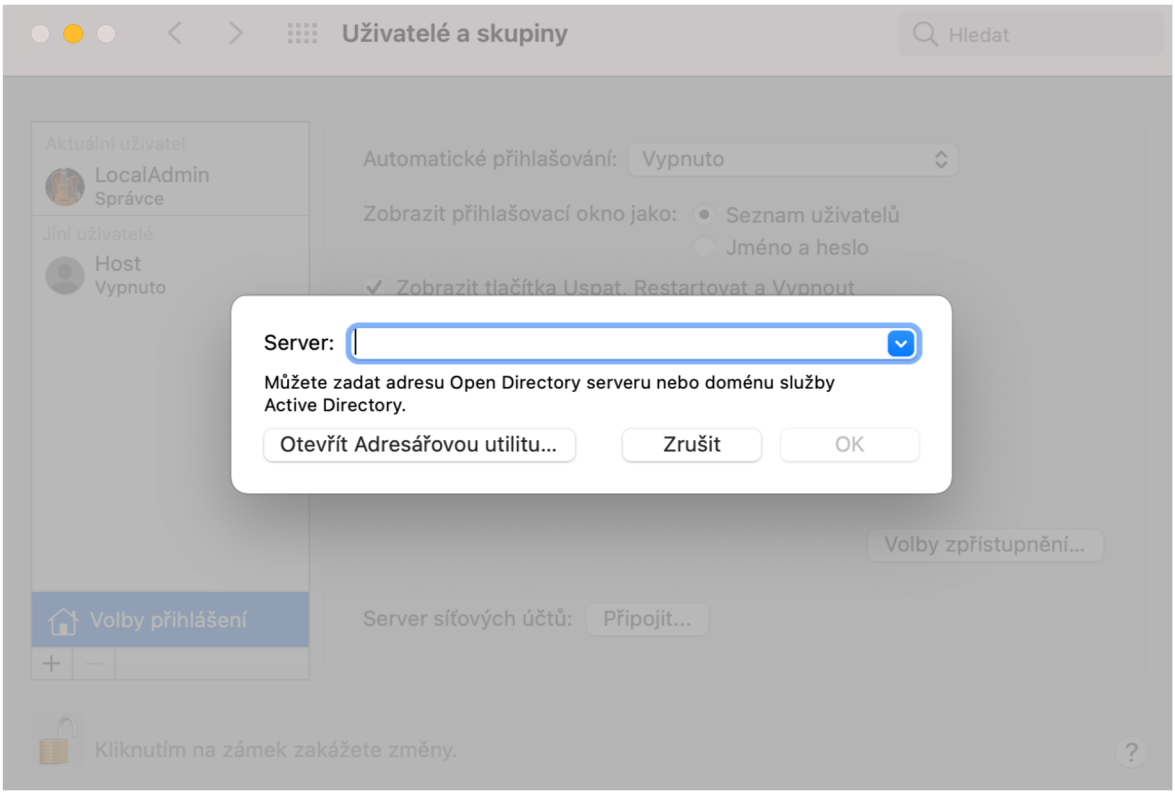
Mac, který chceme integrovat do AD musí být připojen do sítě, kde je AD pomocí Ethernetu, Wi-Fi nebo VPN. A to proto, že musí být využíván DNS server, který umí přeložit doménu, kterou využívá AD. Tento DNS server bývá většinou provozován na Windows serveru, kde je AD.

Dalším specifickým nastavením může být ID počítače, které je možné v průběhu integrace zvolit. Toto ID je následně vidět na straně Windows serveru. Obecně je doporučováno, aby v tomto ID nebyli žádné pomlčky, protože pak může při komunikaci s AD nastat chyba.

Pro mobilní počítače Mac je pak nutné vytvořit napojení, které bude mít vytvořený „Mobilní účet“. Přístupové údaje z AD může uživatel následně používa i v momentě, kdy není připojen do sítě, kde se AD nachází.

4.1.1 Integrace pomocí Předvoleb systému

Nejjednodušší způsob, jak připojit Maca k AD je přes Předvolby systému. Zde v sekci „Uživatelé a skupiny“ můžeme nastavit připojení k AD. Po otevření sekce „Uživatelé a skupiny“ musíme odemknout úpravy heslem administrátora počítače Mac. Toho docílíme klinutím na „zámeček“ vlevo dole. Následně klikneme na „Volby přihlášení“, kde v části „Server síťový účtů“ klineme na tlačítko „Připojit“.



Obrázek 3 - Přímá integrace do AD pomocí Předvoleb systému, zdroj: autor

Poté vyskočí okno, do kterého napíšeme doménu AD a klineme na „OK“. Po navázání komunikace nás systém vyzve zadání jména a hesla administrátora AD. Po úspěšném ověření byl Mac integrován do AD a je možní se přihlašovat k Macu účty z AD.

4.1.2 Integrace pomocí adresářové utility

Integrace pomocí Předvoleb systému je snadná a jednoduchá, ale nenabízí možnosti pokročilého nastavení. V případě, že potřebujeme upřesnit některá nastavení je potřeba využít aplikaci „Adresářová utilita“.

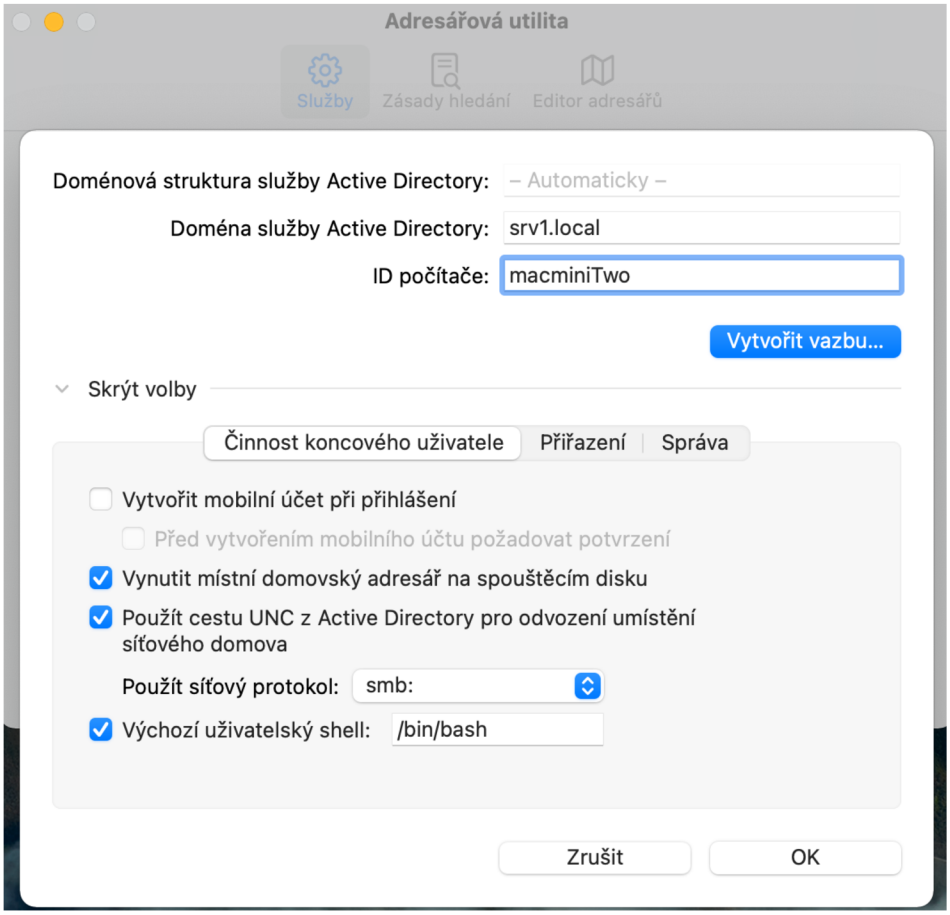
Aplikaci můžeme buď otevřít během integrace přes „Uživatelé a skupiny“ v Předvolbách systému, najít ji pomocí vyhledávač Spotlight či ji otevřít v tomto adresáři */System/Library/CoreServices/Applications* .

Po otevření aplikace je potřeba, stejně jako v případě „Předvoleb systému“, ji odemknout administrátorským heslem pro počítač Mac pomocí zámečku vlevo dole. Po odemčení zvolíme, že chceme realizovat napojení na AD. Dále klikneme na „tužtičku“ vlevo dole, která nám otevře možnosti pro připojení do AD.

V otevřených možnostech připojení zadáme doménu AD. ID počítače je automaticky vygenerované, ale doporučuji ho přepsat tak, aby tvar neměl žádné pomlčky. Pro rozšířené natavení je potřeba kliknout na „Zobrazit volby“. Následně se nám zobrazí tři karty, kde je možné aplikovat další nastavení integrace.

V kartě „Činnosti koncového uživatele“, kterou můžeme vidět na obrázku níže, lze nastavit parametry, které přímo ovlivní možnosti užívání počítače uživatelem. Konrétně jde o tyto volby:

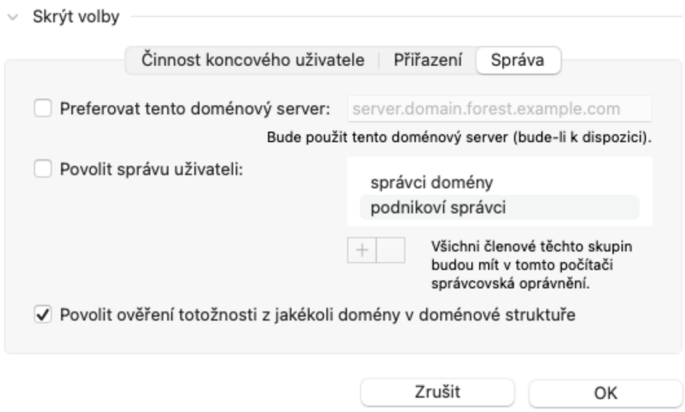
- Vytvoření mobilního účtu (vhodné pro mobilní stroje)
- Vynutit místní domovský adresář
- Zvolit protokol přenosu dat pro domovský adresář
- Nastavit výchozí uživatelský shell



Obrázek 4 - Přímá integrace pomocí Adresářové utility, zdroj: autor

V záložce „Přiřazení“ lze místo dynamicky generovaných atribut pro AD přiřadit vlastní unikátní atributy UID, uživatelský atribut GID a skupinový atribut GID. Ve většině případů se tyto atributy nechávají generovat automaticky, protože pokud jsou zvoleny unikátní atributy a v budoucnu budou změny, tak uživatelé mohou ztratit přístup ke svým souborům.

V poslední záložce „Správa“ lze nestavit preferovaný doménový server (pokud jich je v síti více) a povolit administrátorům z domény spravovat tento Mac.

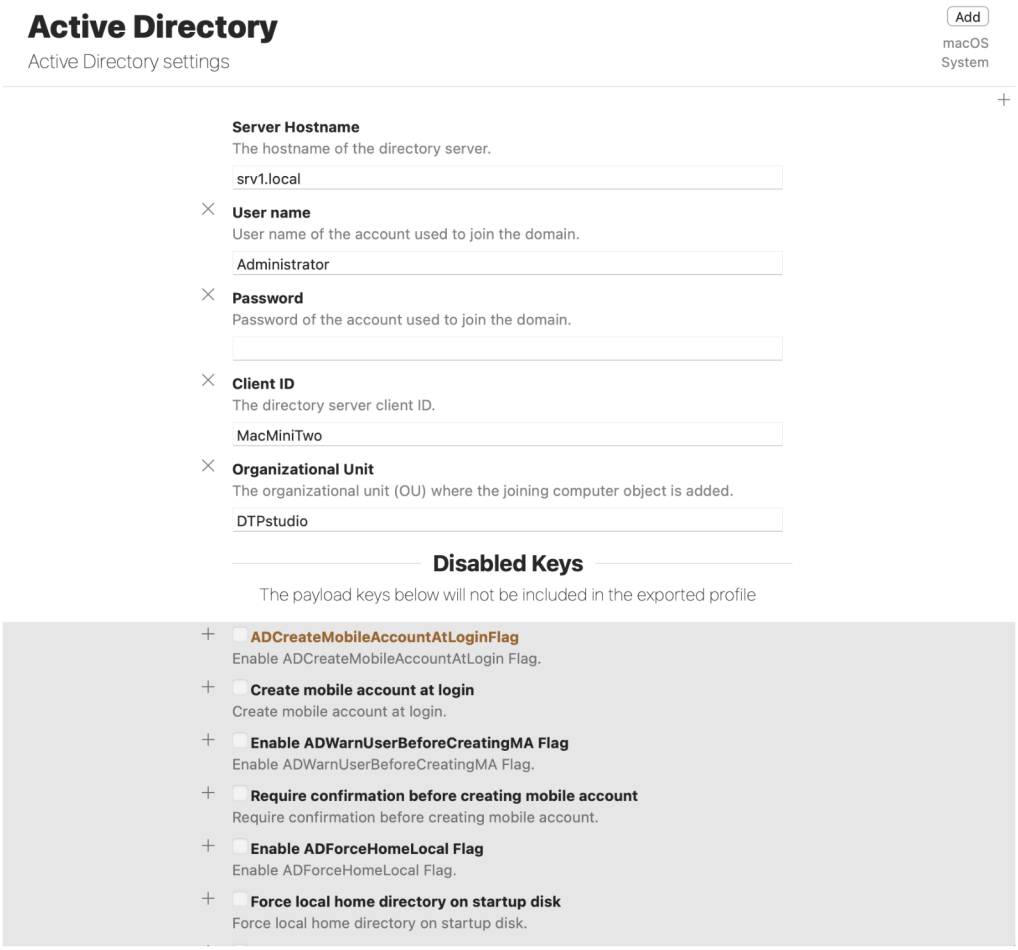


Obrázek 5 - Karta "Správa" v Adresářové utilitě, zdroj: autor

4.1.3 Integrace pomocí konfiguračního profilu

Pokud chceme integrovat větší množství počítačů Mac, tak si můžeme vytvořit konfigurační profil, ve kterém si zvolíme veškeré nastavení, které budeme od přímé integrace požadovat. Následný konfigurační profil pak stačí spustit na daném počítači a automaticky dojde k nastavení našich hodnot.

Je potřeba zdůraznit, že konfigurační soubor je napsán pomocí XML. V tomto případě je tak heslo k AD napsáno přímo v souboru a při neopatrném zacházeni s konfiguračním profilem může dojít k úniku hesla. Tomu lze zabránit šifrováním konfiguračního profilu nebo doručím pomocí MDM.



Obrázek 6 - Vytváření konfiguračního profilu pro přímou integraci do AD v aplikaci ProfileCreator, zdroj: autor

4.2 Nedostatky přímé integrace do AD

Přímá integrace Maců do AD sebou přináší základní nedostatky, na které se narazí v momentě, kdy administrátor sítě bude chtít spravovat počítače Mac podobně jako počítače s Windows. V následujících bodech jsou tyto nedostatky vyjmenovány:

- Nastavení politik
- Distribuce softwaru a správa aktualizací

Tyto nedostatky vyplývají ze samého principu přímé integrace, kdy plugin AD v macOS využije zabezpečovací protokol Kerberos a LDAP k identifikaci uživatelů a skupin. Mac není schopen využívat Group Policy, které se v AD běžně používají pro nastavení politik na počítačích se systémem Windows. Tyto nedostatky je tedy potřeba řešit pomocí aplikací či služeb třetích stran.

4.2.1 Nedostatečná spolehlivost

Kromě nedostatků, které vyplývají ze samotného principu přímé integrace Macu do AD, jsem při krátkodobém testování a dlouhodobém provozu objevil problémy se spolehlivostí přímé integrace. Problémy se týkali většinou přihlášení, které se nepovedlo bez objektivní příčiny nebo po změně hesla uživatele na počítači Windows. Narazil jsem také na problém, kdy Mac ztratil připojení do AD po upgradu systému i když Adresářová utilita nebo Systémové preference ukazovali spojení jako aktivní.

Pro zjištění, jak jsou tyto problémy časté jsem rozhodl otestovat jejich četnost. Na základě výsledků testování, by mělo jít provést rozhodní zda je výhodné přímou integraci využívat.

4.2.1.1 Problémy s přihlášením

Pro testování problému s přihlášením jsem zvolil Mac Mini, který v síti funguje jako „veřejný“ počítač pro každého, kdo potřebuje k nějaké činnosti macOS. K počítači jsem na jeden měsíc přiložil papírový dotazník a instruoval všechny uživatele, aby ho po přihlášení vyplnili. Dotazník sledoval tyto údaje:

- Uživatelské jméno
- Přibližný čas přihlášení
- Informace o úspěšném přihlášení ve formě ANO/NE
- Počet pokusů o přihlášení

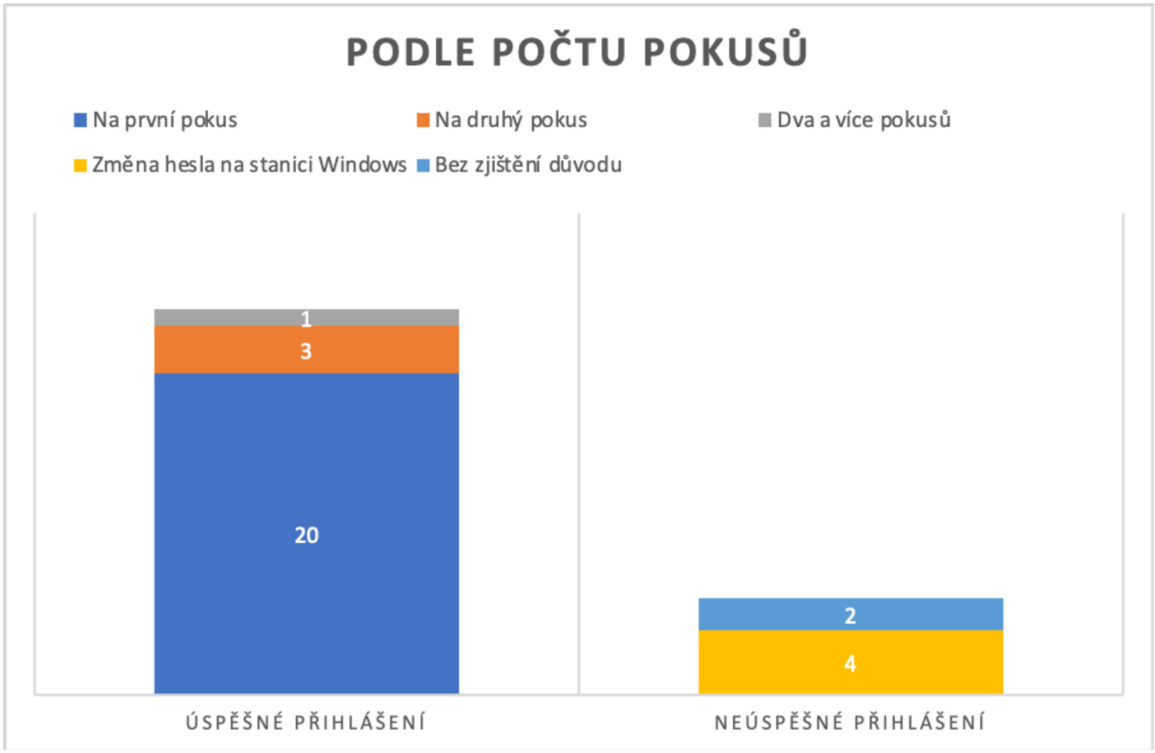
4.2.1.1.1 Výsledky šetření

Záznam	Hodnota záznamu
Počet uživatelů	9
Počet přihlášení	30
Počet úspěšných přihlášení	24
Počet úspěšných přihlášení	6

Tabulka 1 - Záznam o úspěšnosti přihlášení do AD

V průběhu jednoho měsíce se u počítače vystřídalo 9 uživatelů, kteří celkem provedli 30 pokusů o přihlášení ke svým účtům v AD. Z těchto 30 přihlášení bylo 24 úspěšných, jedná se tedy o úspěšnost 80 %.

Níže v grafu jsou pak znázorněni počty pokusů uživatelů pro úspěšné přihlášení. Lze vyčíst, že drtivá většina přihlášených (20 přihlášení) byla úspěšná na první pokus. Ve třech případech byl pokus o přihlášení úspěšný až na druhý pokus a v jednom případě bylo potřeba více pokusů pro přihlášení. Dále můžeme vyčíst, že 4 neúspěšná přihlášení byla způsobena změnou hesla uživatele na stanici Windows.



Graf 1 - Zobrazení počtu pokusů o přihlášení do AD

Ve dvou případech, kdy se nepodařilo dohledat důvod neúspěšného přihlášení se ukázalo, že tento problém měl pouze jediný uživatel, a to v jeden a ten samí den v rozmezí dvou hodin. Po rozhovoru s uživatelem se ukázalo, že zapomněl heslo. Po té co si vzpomněl se přihlásil normálně.

Z výsledků lze konstatovat, že míra spolehlivosti přihlášení uživatele není nejlepší, ale v běžném provozu s ní lze fungovat. Pokud ovšem dojde ke změně hesla uživatele na pracovní stanici Windows, tak lze předpokládat, že může dojít k neúspěšnému přihlášení na počítači Mac.

4.2.1.2 Ztráta napojení na AD při upgradu macOS

Přo efektivní zjištění, jak četně se může objevovat problém ztráty připojení k AD jsem rozhodl využít program VMware Fusion, který umožňuje na Macu vytvářet a provozovat virtuální počítače. Vytvořil jsem virtuální disk s macOS 10.15 Catalina (verze macOS, která byla před verzí 11 Big Sur), který jsem si zazálohoval, aby bylo možné virtuální počítat snadno obnovit.

Tento virtuální počítat jsem následně pomocí Adresářové utility přidal do AD a po otestování funkčnosti jsem spustil instalaci nové verze macOS 11 Big Sur. Po dokončení instalace jsem zakontroval funkčnost napojení na AD. Podobně jako u testování spolehlivosti přihlášení jsem pomocí papírové dotazníku vedl následující údaje:

- Číslo pokusu
- Informaci o funkčnosti napojení ANO/NE
- Stav funkčnosti, který eviduje macOS

Pokus byl ukončen smazáním virtuálního disku a obnovením původního virtuálního disku pro opakování pokusu.

4.2.1.2.1 Výsledky šetření

Záznam	Hodnota záznamu
Počet pokusů	10
Počet úspěšných pokusů	4
Počet neúspěšných pokusů	6
Počet evidencí o funkčním propojení v macOS	10

Tabulka 2 - Záznam úspěšnosti fungování integrace do AD po upgradu systému

Z výsledku šetření je patrné, že úspěšných pokusů bylo pouze 40 %. Zajímavějším zjištěním je fakt, že macOS vždycky ukazoval, že připojení do AD je funkční. To může vést ke zmatení administrátora sítě, který může spojení považovat za aktivní.

Je proto potřeba počítat s tím, že po větším upgradu macOS, při kterém je požadován restart počítače, může nastat problém s napojením do AD a nespoléhat na tvrzení macOS, že napojení je funkční.

4.3 Možnosti řešení nedostatků

Pro řešení nedostatků, které vyplývají z přímé integrace do AD je důležité poskytnou administrátorovi sítě počítač Mac, který může mít u sebe v kanceláři nebo v serverovně. Tento Mac je důležitý pro snadnou virtualizaci systému macOS, kde je zapotřebí zkoušet řešení nedostatků na konkrétní síti s AD. Dále na něm lze provozovat aplikace pro macOS, které usnadní správu ostatních počítačů Mac. Může být také využíván jako server pro ostatní počítače Mac, které k němu mohou přistupovat. To je vhodné například pro aplikaci Munki nebo Apple Profile Manager. Může se jednat o jakýkoliv Mac, který má minimálně tyto parametry:

- Velikosti operační paměti: 16 GB
- Šesti jádrový procesor Intel
- 1 TB SSD
- Model uvedený v roce 2018

4.3.1 Řešení spolehlivosti napojení do AD

Problémy se spolehlivostí jsou způsobovány pluginem pro AD, který přímo do macOS dává Apple. Tyto problémy přetrvávají dlouhodobě a s novými verzemi macOS se nic nemění. Je tedy pravděpodobné, že jde o věc, kterou Apple neřeší a řešit ani nebude.

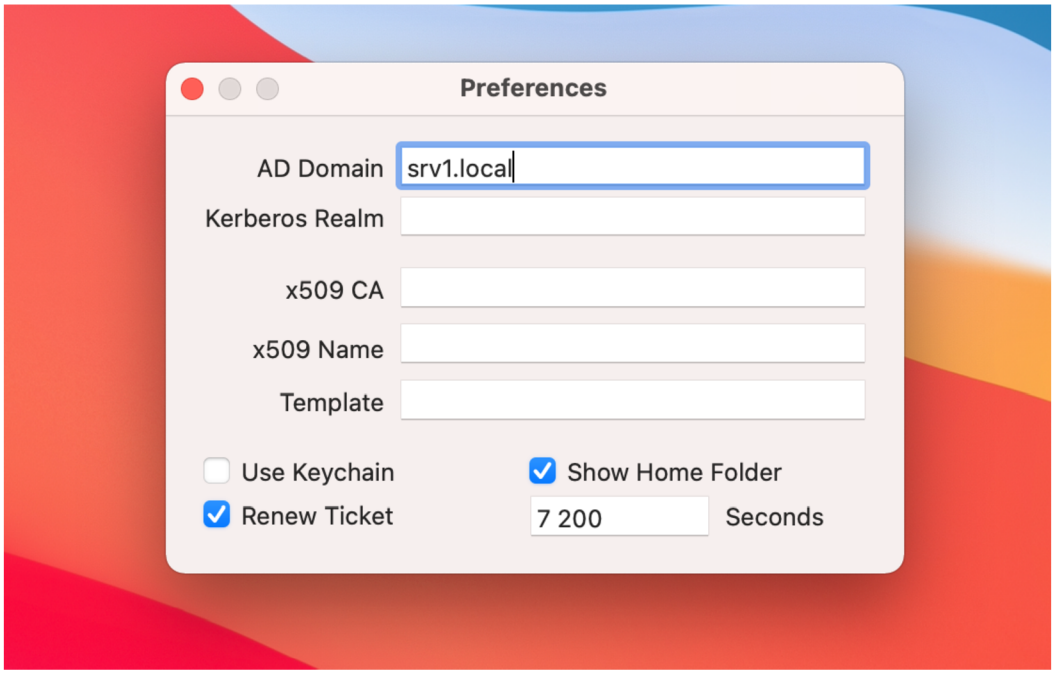
Jediným způsobem, jak vyřešit nespolehlivost je nevyužívat možnosti přímé integrace Macu do AD. Pro připojení do AD je tak vhodné použít aplikace NoMAD či NoMAD Login, které zajistí komunikaci s AD bez toho, aniž by do ní byl Mac přímo integrován.

Pro úspěšné nasazení těchto aplikací je důležité uvědomit si, že uživatel na Macu využívá lokální účty a aplikace NoMAD slouží k načtení platnosti hesla, změny hesla a připojení domovské složky v AD. Účet, kterým je uživatel na Macu přihlášen je tedy oddělen od účtu v AD.

4.3.1.1 Využití a instalace aplikace NoMAD

Aplikace NoMAD se hodí pro Mac, který má převážně jednoho stálého uživatele nebo Macy, které využívají externí entity (např.: vlastník počítače není firma provozují AD). NoMAD zde funguje jako synchronizační prvek mezi dvěma oddělenými účty. Lokálním a tím v AD.

Používání je velmi jednoduché, protože aplikaci stačí nainstalovat a následně zadat doménu AD a případné základní požadavky jako zobrazení domovského adresáře nebo užívání klíčenky pro synchronizaci hesel.

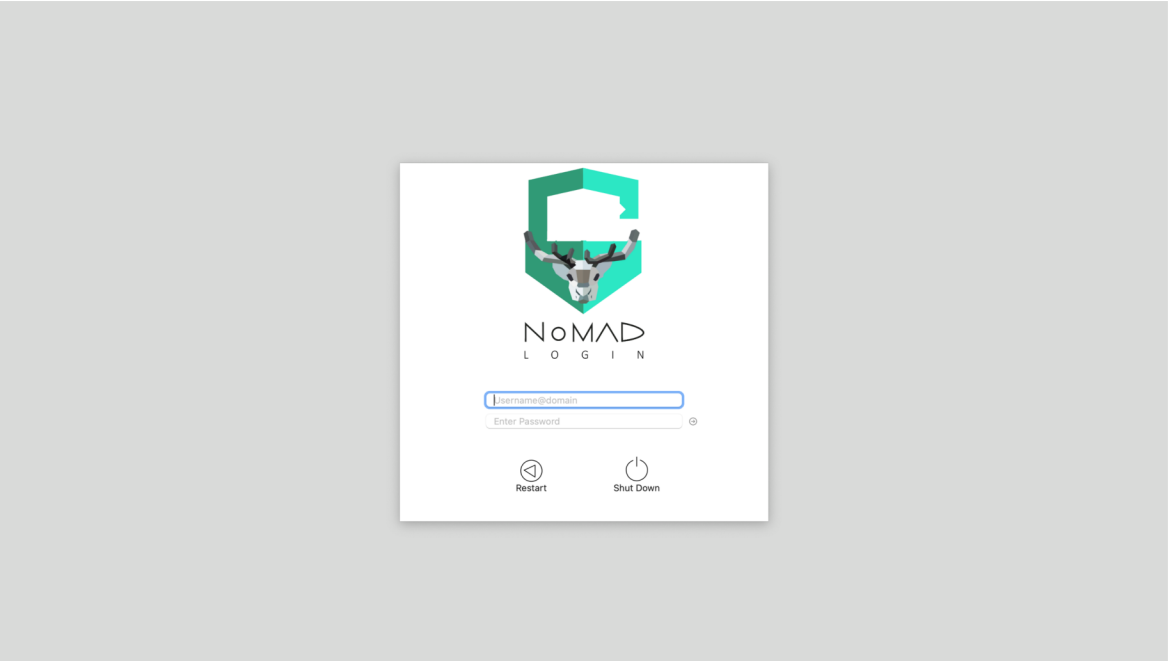


Obrázek 7 - Nastavení aplikace NoMAD, zdroj: autor.

NoMAD také nabízí možnosti nastavení pro AD, kde se využívá certifikační autorita podle standardu X.509. Pokud není standard použit nechají se políčka volná a okno „Preferences“ se zavře „červeným kroužkem“. Nastavení není potřeba ukládat. Pokud je AD dostupná, tak po tomto kroku lze využívat aplikaci NoMAD. Veškeré nastaven také lze provést pomocí konfiguračního profilu či využitím skriptu.

4.3.1.2 Využití a instalace aplikace NoMAD Login

Zatím co NoMAD je vhodný pro uživatele, kteří pracují stále s jedním strojem nebo pro externí entiny, tak NoMad Login je vhodné používat na zařízeních, které využívá více uživatelů. Používání je podobně snadné jako v případě NoMAD, kdy aplikací stačí pouze nainstalovat a bez nutnosti dalšího nastavení lze hned používat.



Obrázek 8 - Přihlašovací obrozvka po instalaci apliakce NoMAD Login, zdroj: autor

Pomocí konfiguračního profilu pak jdou nastavit specifická nastavení pro konkrétní síť AD nebo organizaci. Například se může jednat:

- Nastavení spuštění skriptů
- Úpravy UI vzhledu
- Nastavení výpisu dostupných domén
- Zákaz konkrétních lokálních účtů
- Zákaz nebo povolení účtu hosta
- Zákaz nebo povolení demobilizace účtů

Další možnosti nastavení lze najít v [] nebo v aplikaci ProfileCreator, kde lze vytvářet konfigurační soubory pro NoMAD Login.

4.3.2 Řešení distribuce softwaru a správy aktualizací

Pro řešení distribuce softwaru lze použít aplikaci Munki, kterou můžeme nasadit na libovolný počítač, kde může běžet webserver. V našem případě ji budeme instalovat na počítač Mac, který má administrátor AD k dispozici.

4.3.2.1 Instalace Munki

Nejdříve je potřeba stáhnout aktuální verzi aplikace Munki, která je distribuovaná jako softwarový balíček. Tuto aplikaci jednoduše nainstalujeme jako každou jinou. Po instalaci je potřeba postupovat podle návodu na Githubu aplikace [].

Návod nás provede následujícími kroky:

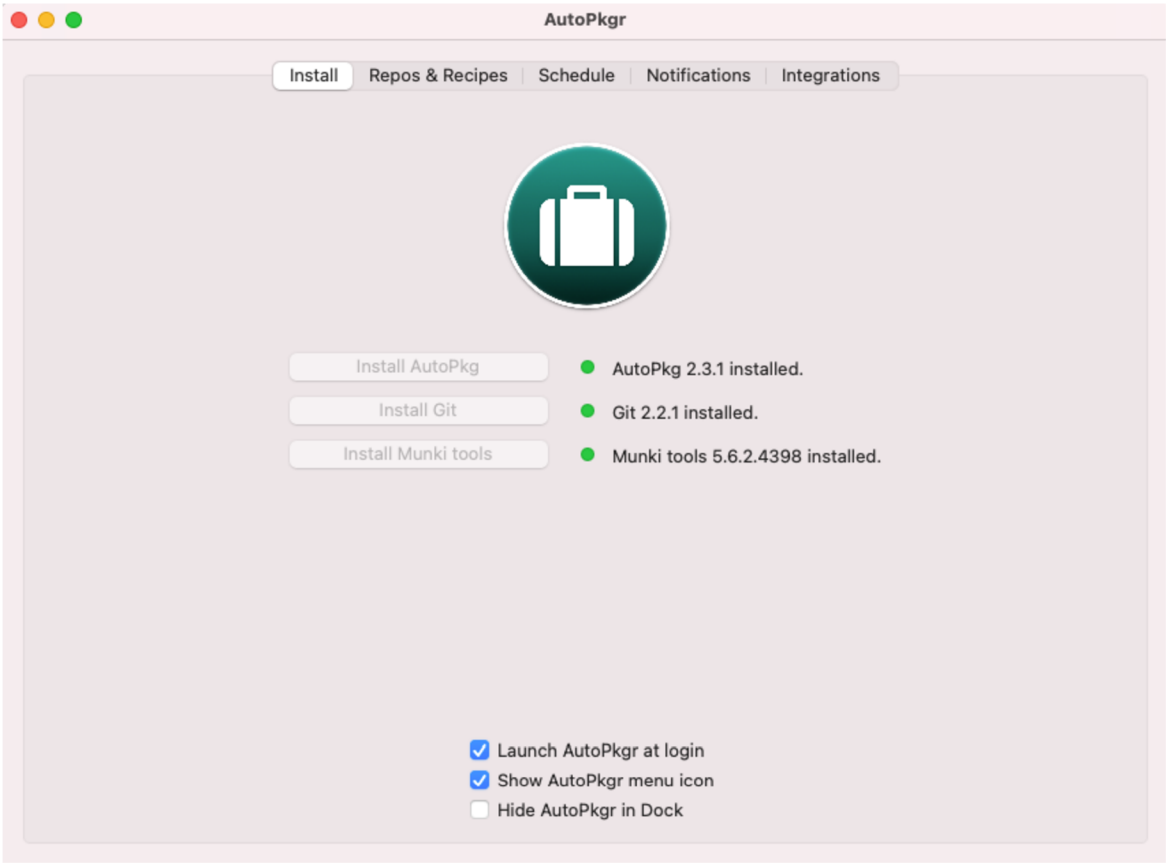
- Vytvoření struktury adresářů pro repositář
- Aktivování serveru Apache 2
- Nastavení Munki repo
- Importování aplikace Firefox pro otestování
- Vytvoření katalogu
- Vytvoření manifestu pro klienty
- Nastavení klienta pro komunikaci s Munki

4.3.2.2 Správa pomocí AutoPkgr

Pro snadnější správu lze použít aplikaci AutoPkgr, která se postará o instalaci frameworku AutoPkg, Gitu a zvládne také aktualizovat aplikaci Munki. Pro integraci s aplikací Munki je potřeba v záložce „Integrations“ nastavit adresu adresáře, který využívá Munki.

Pomocí této aplikace můžeme následně ovládat framework AutoPkg, který nám umožní do Munki importovat aplikace, pravidelně kontrolovat aktuálnost a stahovat aktualizace. Není tak potřeba využívat proto toto nastavení terminál a grafické rozhraní.

Výběr aplikací, které chceme mít v Munki se provádí přes záložku „Repos & Recipes“, kde se nachází repositáře, které umístili ostatní uživatelé na Github. Nachází se zde všechny aplikace, které jsou běžně v provozu. Od všech internetových prohlížečů přes aplikace MS Office až po aplikace od společnosti Adobe. Pokud chceme přidat nějakou aplikaci do Munki stačí v seznamu najít její instalaci, která končí na koncovkou .munki a následně ji „zaškrtnout“.

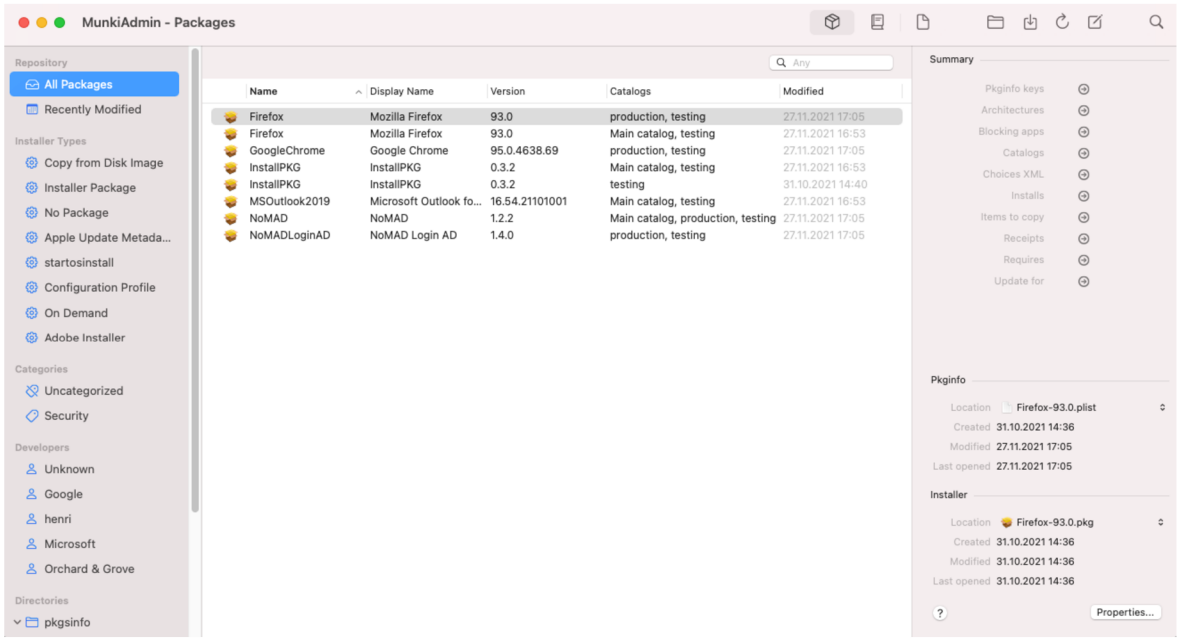


Obrázek 9 - Aplikace AutoPkgr, zdroj: autor

4.3.2.3 Nastavení pomocí MunkiAdmin

Zatímco aplikace AutoPkgr nám umožnila vyhnout se používání terminálu pro importování aplikací do Munki, tak MunkiAdmin nám umožní ovládat přes grafické rozhraní i další funkce Munki. Konkrétně jde o:

- Přehled aplikací v Munki
- Vytváření a editace katalogů
- Vytváření a editace manifestů



Obrázek 10 - Aplikace MunkiAdmin, zdroj: autor

4.3.2.3.1 Přehled aplikací

V kartě přehledu aplikací vidíme všechny instalační balíčky, který jsou importovány do Munki. Vidíme jejich název, verzi, datum modifikace a v jakých katalogách je máme. Pro snazší přehled můžeme aplikace třídit podle druhu instalace, kategorie a vývojáře.

4.3.2.3.2 Vytváření katalogů

V záložce vytváření katalogů vidíme všechny existující katalogy. Můžeme je snadno editovat a vytvářet nové. Každé nasazení programu Munki by mělo obsahovat minimálně dva katalogy:

- Testovací
- Produkční

Toto rozdělení nám umožní nově přidané aplikace nejdříve otestovat před nasazením pro uživatele. Testovací krok je nutný a silně nedoporučuji se mu vyhýbat.

4.3.2.3.3 Vytváření manifestů

V neposlední řadě můžeme vytvářet manifesty, kterými specifikujeme, jaký software a z kterých katalogů se má nainstalovat na konkrétních stanicích. Dále můžeme nastavit odinstalaci specifického softwaru a volitelný software pro koncové uživatele.

Pro specifikováni, na kterých stanicích má být manifest použit můžeme využít následující identifikátory:

- Hostname
- Architektura procesoru
- Verze macOS
- Model Macu
- Sériové číslo Macu
- Druh Macu
- Konkrétní build macOS
- IP adresu Macu

4.3.3 Řešení nastavení politik

Jako řešení těchto nedostatků se v minulosti používala Dual Directory (Duální adresářová služba), která je také známá jako „Zlatý trojúhelník“. Toto řešení spočívalo v provozu AD a OD najednou, kdy Mac byl integrován do obou těchto služeb. Společně s dalšími službami v macOS Server byli nastavovány politiky a další potřebná nastavení. Jako příklad mohu uvést aplikace Workgroup Manager, která byla součástí macOS server.

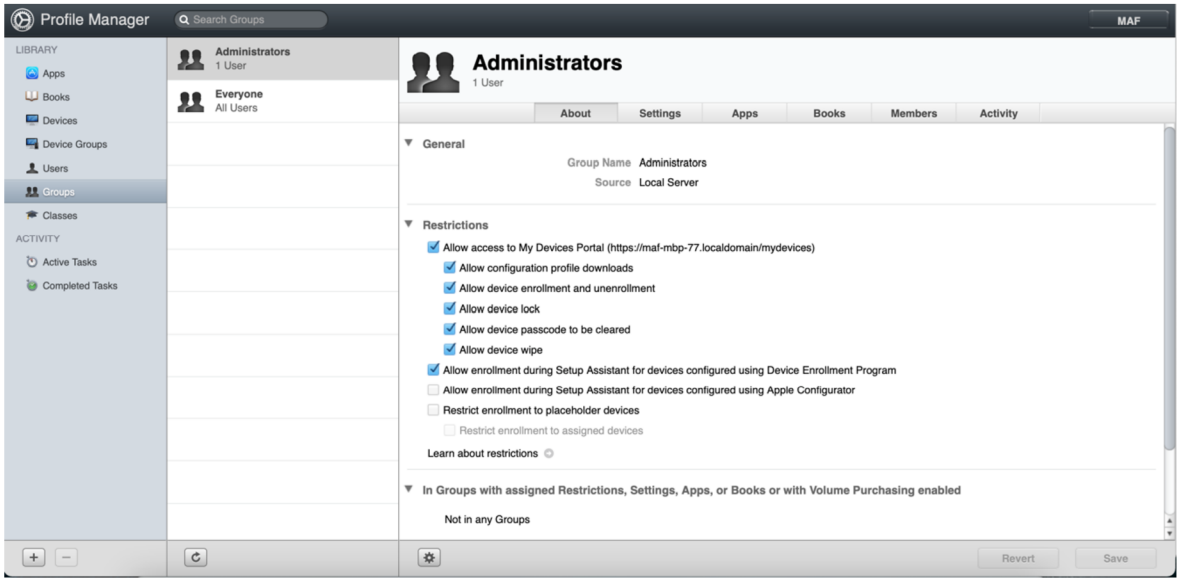
Dnes sice OD stále existuje, ale třeba již zmíněná aplikace Workgroup Manager není podporována. Apple totiž tlačí na využívání konfiguračních profilů a služby MDM, které ve své podstatě nahrazují již nepodporované možnosti správy. Tento způsob správy zařízení je běžný u mobilních zařízeni iPhone a iPad a na Macu se stává realitou, bez které se v případě nastavení politik nelze obejít.

Toto řešení sebou navíc přináší výhody, protože není potřeba aby spravované zařízení bylo připojené do firemní sítě, kde byl konfigurační profil vytvořen. To je značná výhoda oproti Group Policy v AD, kde dané zařízení musí být součástí AD.

4.3.3.1 Vytváření konfiguračního profilu

Konfigurační profil lze vytvářet pomocí různých aplikací nebo si ho lze napsat. Aplikace jsou buď samostatné nebo součástí služby MDM. Příkladem samostatné aplikace

může být open source aplikace ProfileCreator, která kromě standardních parametrů pro macOS a iOS umí vytvářet konfigurační profily, které umí nastavit aplikace třetích stran jako jsou NoMAD, NoMAD Login nebo Munki. Příkladem vytváření konfiguračního profilu aplikací, která je součástí služby MDM může být Apple Profile Manager, který je současní Serverové aplikace pro macOS.



Obrázek 11 - Apple Profile Manager, zdroj: autor

Při vytváření je důležité uvědomit si, jak bude profil aplikován. Můžeme totiž vyvářet profily pro jednotlivé uživatele nebo na úroveň celého systému. Pomocí konfiguračního profilu lze nastavit prakticky jakékoliv systémové nastavení nebo nastavení konkrétní aplikace, která je podporována aplikací vytvářející konfigurační profil.

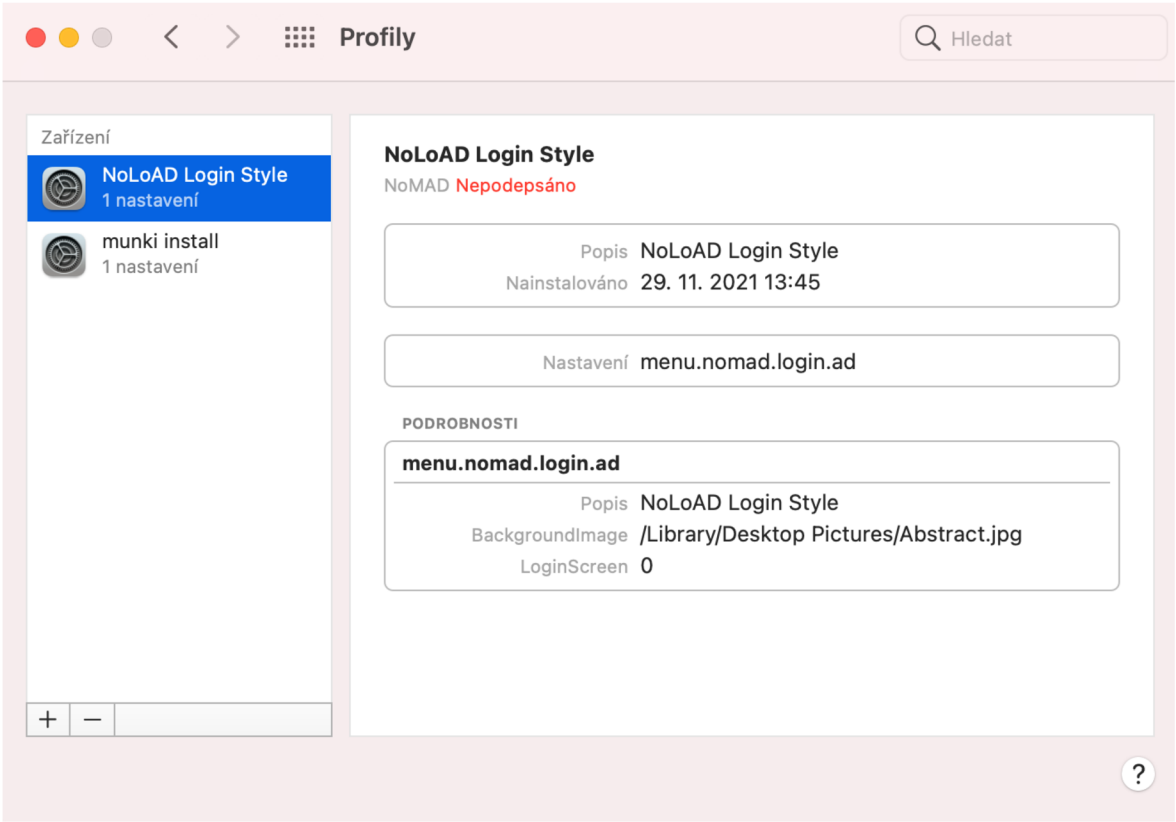
4.3.3.2 Ruční instalace profilu

Jde o základní způsob instalace konfiguračního profilu, který spočívá v otevření profilu na daném zařízení. Po proběhnutí instalace lze úspěšnost zkontrolovat v Předvolbách systému, kde se nově objeví záložka „Profily“. Na tomto míst lze také profily odstraňovat.

Abychom zabránili odebrání profilu, který byl ručně naistalován, uživatelem je potřeba ošetřit odstranění zadáním hesla. Aby nemohlo dojít k úniku hesla je zapotřebí

konfigurační profily nezveřejňovat nebo ho šifrovat (neplatí při doručování pomocí MDM).

Tento způsob instalace je vhodný při nasazení malých jednotek Maců a malého množství bezpečnostních politik. Při větším zastoupení počítačů Mac se tento způsob instalace profilů stává nepřehledný a je následně vhodné použít spíše službu MDM. Ovšem hlavní nevýhodou je, že v případě potřeby změny nastavení je potřeba přijít ke každému Macu zvlášť a profil odebrat a poté přidat nový profil. To může výrazně prodloužit čas na nasazení nových politik.



Obrázek 12 - Aktivní konfigurační profily zobrazení v Předvolbách systému, zdroj: autor

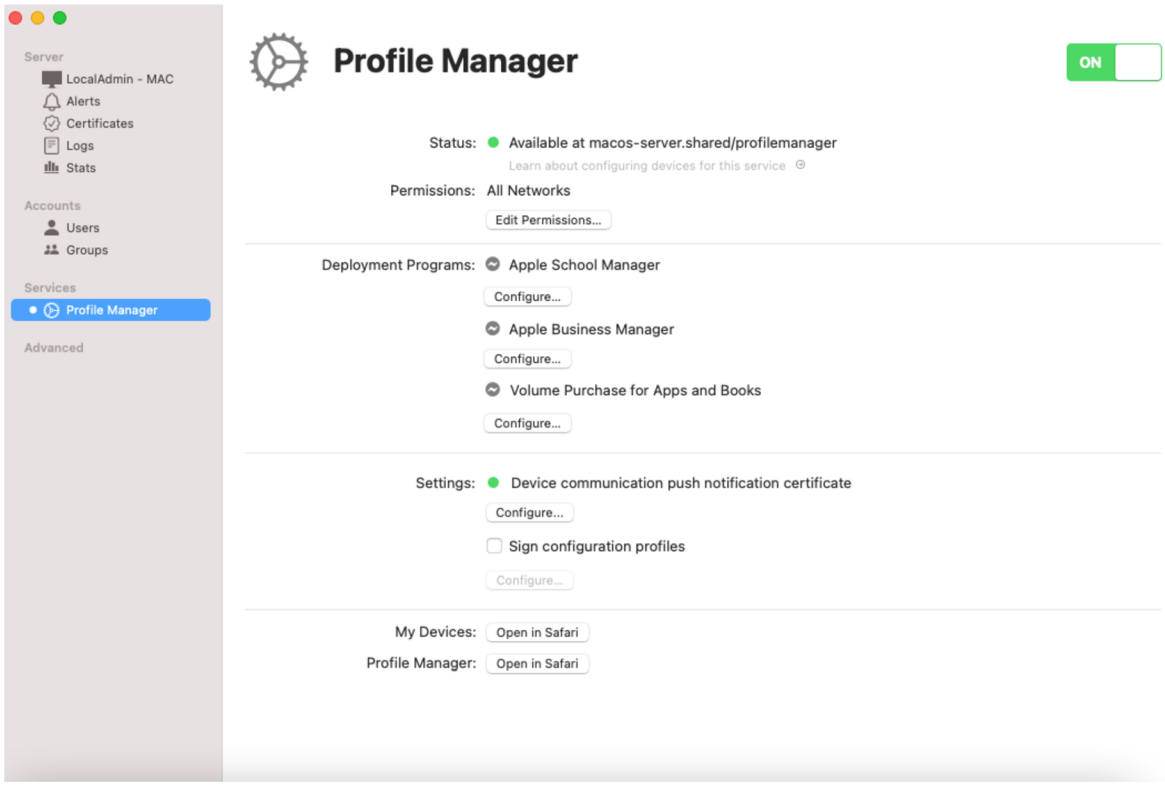
4.3.3.3 Distribuce a hromadná instalace konfiguračních profilů

Pokud chceme konfigurační profily distribuovat automaticky a hromadně je potřeba používat službu MDM jakou je například Apple Profile Manager (slouží pro obsluhu pouze zařízení a operačních systémů značky od Applu). Konfigurační profily umožňuje distribuovat pomocí služby Apple Push Notifications, do které se přihlásíme přes Apple ID. Je vhodné pro tyto účely nepoužívat své soukromé Apple ID.

Pomocí Profile Manageru můžeme distribuovat profily pro konkrétní zařízení či uživatele, kdy stačí aby daný objekt byl pouze připojen k internetu. Profily lze ve službě vytvářet nebo nahrávat profily vytvořené v jiné aplikaci. Profily, které jsou takto instalované na zařízeních můžeme vzdáleně buď upravit nebo smazat.

Službu lze také propojit s programy Applu podporující hromadnou správu zařízení. Můžeme tak distribuovat profily na zařízení, které byli teprve koupeny nebo aktivovány. Uživateli se během prvotního nastavení stáhnou konfigurační profily a zařízení se nastaví samo. Není tedy třeba, aby s ním uživatel šel ke správci sítě. Využívání těchto služeb přináší i výhody v podobě registrovaného vlastnictví dané organizace a správce MDM může zařízení smazat i přes specifická nastavení ze strany uživatele. Další výhodou je, že profily distribuované skrz MDM není potřeba dopředu šifrovat.

V případě potřeby lze zvolit i jiné řešeny MDM, které je dostupné na trhu. Pro některé organizace, které provozují stovky Maců a další stovky jiných zařízení Apple nebo postupně chtějí opouštět od využívání AD je naopak vhodné vybrat řešení MDM, které podporuje další operační systémy nebo konkrétní služby, které organizace potřebuje.



Obrázek 13 - Nastavení Apple Profile Manageru v Serverové aplikaci macOS, zdroj: Autor

5 Výsledky a diskuse

5.1 Doporučený způsob integrace do AD

Pokud je to možné, tak je silně preferováno nepoužívat plugin pro AD, který je v macOS. Přímá integrace sice prokazuje známky funkčnosti, ale z dlouhodobého hlediska představuje problémový element, který kromě napojení na účet uživatele nepřináší žádné výhody v podobě správy zařízení nebo nastavení bezpečnostních politik. I přímé integraci je potřeba využívat některé aplikace či služby třetích stran.

Pro připojení do AD je vhodné používat aplikace NoMAD nebo NoMAD Login, které zajistí přehlášení do AD bez nutnosti integrace. Pomocí konfiguračních profilu jdou nastavit všechny možná nastavení těchto aplikací a tím usnadnit nastavení. Tyto aplikace lze používat samostatně nebo v kombinaci.

5.2 Doporučení způsobu správy počítačů Mac

Počítače Mac by neměli být vynechány ze správy zařízení. Jako vhodný způsob správy zařízení se ukázaly konfigurační profily, které dokážou nahradit Group Policy v AD. Profily lze vytvářet na úroveň systému i uživatele. Administrátor si tedy může rozdělit, jak politiky bude aplikovat.

Konfigurační profily můžeme instalovat ručně na daném zařízení. V případě profilů, které se vztahují na celé zařízení lze snadno tyto politiky aplikovat ručně, protože platí pro všechny uživatele. Konkrétní uživatelské profily lze pak instalovat pouze po přihlášení daného uživatele. Stejný postup se musí aplikovat i při odebírání profilu. Případné změny politik se musí aplikovat ručním odebráním profilu a znovu nainstalovat aktualizovaný profil.

Pokud je to možné, tak silně doporučuji využívat některou ze služeb MDM, která zajistí hromadnou distribuci konfiguračních profilů. Pro pouhé nasazení počítačů Mac lze zvolit Apple Profile Manager, který je součástí aplikace Server v macOS. V kombinacemi s aplikacemi jako je Munki lze pak spravovat počítače Mac celkem snadno.

V momentě, kdy začne převažovat zastoupení Maců v AD a je možnost investovat do modernizace, tak je doporučováno zvolit službu MDM od třetí strany. Služby MDM třetích strach obvykle podporují macOS, Windows i Linux a je možné přesunout AD do ústraní a spoléhat na MDM na všech stanicí bez ohledu na operační systém.

Ostatně tento krok se nyní velmi často provádí z důvod nejrůznějších „home officů“ způsobné pandemií nemoci COVID 19.

5.3 Mac na oddělení správce sítě

Je doporučováno, aby v kanceláři, kde je administrátor AD byl nasezen alespoň jeden počítač Mac. Na tomto Macu by měli být nainstalovány všechny aplikace či frameworky pro macOS, které usnadní správu ostatních Maců. Dále umožní snadnou virtualizaci systému macOS. Je preferováno, aby pro testování změň v nastavení správy počítačů Mac byl využíván virtuální stroj.

6 Závěr

V první části bakalářské práce byl popsán pojem firemní síť a byli definovány základní potřeby takovéto sítě z hlediska zajištění funkčnosti sdílení informací a dat mezi jednotlivými zařízeními, uživateli a skupinami. Dále byly popsány základní principy fungování adresářových služeb a AD. Byla představená konkurenční OD od Applu a uveden důvod proč by se neměla používat. Dále byli způsoby, jak pracovat s Macem ve firemní prostředí, a to včetně představení služby MDM a programů Applu, které mohou MDM využívat. V poslední kapitole první části práce byli představeny aplikace třetích stran, které mohou být použity pro řešení nedostatků přímé integrace do AD.

V praktické části bylo ukázáno, jak postupovat při přímé integraci počítačů Mac do AD. Byli definovány nedostatky toho řešení, které vyplývali z možností funkce přímé integrace. Dále byli ukázány nedostatky, které odhalil provoz počítačů Mac v síti AD. Nedostatky, které byli odhaleny během provozu podstoupili šetření, aby se ukázalo, jak moc jsou časté.

Byl ukázán postup, jak vyřešit nespolehlivost přímé integrace počítačů Mac do AD za pomocí aplikací NoMAD a NoMAD Login. Následně byli ukázány postupy pro distribuci softwaru za využití nástroje Munki. Pro vyřešení problému nastavením politik bylo popsáno zacházení s konfiguračními soubory a používání MDM.

7 Seznam použité literatury

1. CHARLES EDGE, William Smith. *Enterprise Mac Administrators Guide*. 2. 2015 [cit. 24.9.2021]. ISBN 9781484217061.
2. William R. Stanek. Active Directory. 2013 [cit. 24.8.2021]. ISBN 9788025125557
3. Pavlicek J., Pavlickova P., Naplava P. *Measures of quality in Business Process Modeling*. 2019.

8 Seznam použitých zdrojů

4. What is an Enterprise Network? - Definition from Techopedia. Techopedia: Educating IT Professionals To Make Smarter Decisions [online]. [cit. 30.7.2021]. Dostupné z: https://www.techopedia.com/definition/7044/enterprise-network

5. What is Network Infrastructure? - Definition from Techopedia. Techopedia: Educating IT Professionals To Make Smarter Decisions [online]. [cit. 30.7.2021]. Dostupné z: https://www.techopedia.com/definition/16955/network-infrastructure

6. Adresářové služby a LDAP < články -> SAMURAJ-cz.com. SAMURAJ-cz.com - počítačové sítě, Cisco, Microsoft, VMware, administrace [online]. [cit. 1.8.2021]. Dostupné z: https://www.samuraj-cz.com/clanek/adresarove-sluzby-a-ldap/

7. Active Directory komponenty - domain, tree, forest, site < články -> SAMURAJ-cz.com. SAMURAJ-cz.com - počítačové sítě, Cisco, Microsoft, VMware, administrace [online]. [cit. 1.8.2021]. Dostupné z: https://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/

8. Integrace systému macOS se službou Microsoft Active Directory - Podpora Apple (CZ). Official Apple Support [online]. Všechna práva vyhrazena. [cit. 2.8.2021]. Dostupné z: https://support.apple.com/cs-cz/guide/deployment-reference-macos/iorbeda89d1d/web

9. Nastavení mobilních uživatelských účtů pomocí aplikace Adresářová utilita na Macu - Podpora Apple (CZ). Official Apple Support [online]. Copyright © 2021 Apple Inc. Všechna práva vyhrazena. [cit. 2.8.2021]. Dostupné z: https://support.apple.com/cs-cz/guide/directory-utility/diruc37c9dad/6.2/mac/12.0

10. Přiřazení ID skupiny, primárního GID a UID k atributu Active Directory v Adresářové utilitě na Macu - Podpora Apple (CZ). Official Apple Support [online]. [cit. 3.8.2021]. Dostupné z: https://support.apple.com/cs-cz/guide/directory-utility/diru0f42005a/6.2/mac/12.0

11. Nastavení domovských složek pro uživatelské účty pomocí aplikace Adresářová utilita na Macu - Podpora Apple (CZ). Official Apple Support [online]. [cit. 3.8.2021]. Dostupné z: https://support.apple.com/cs-cz/guide/directory-utility/diru31ab8054/6.2/mac/12.0
12. Co je Adresářová utilita - Podpora Apple (CZ). Official Apple Support [online].. [cit. 3.8.2021]. Dostupné z: https://support.apple.com/cs-cz/guide/directory-utility/xsvroddu001/mac
13. Přehled MDM pro zařízení Apple - Podpora Apple (CZ). Official Apple Support [online]. [cit. 4.8.2021]. Dostupné z: https://support.apple.com/cs-cz/guide/mdm/mdmbf9e668/web
14. Úvod do integrace a nastavení - Podpora Apple (CZ). Official Apple Support [online]. [cit. 4.8.2021]. Dostupné z: https://support.apple.com/cs-cz/guide/deployment-reference-macos/apdb421c7f34/web
15. Products | NoMAD. NoMAD | Keep the functionality, lose the bind [online]. [cit. 5.8.2021]. Dostupné z: https://nomad.menu/products/
16. Overview | NoMAD. NoMAD | Keep the functionality, lose the bind [online]. [cit. 4.8.2021]. Dostupné z: https://nomad.menu/help/130/
17. README.md · main · orchardandgrove-oss / NoMADLogin-AD · GitLab. [online]. Dostupné z: https://gitlab.com/orchardandgrove-oss/NoMADLogin-AD/-/blob/main/README.md
18. preferences · Wiki · orchardandgrove-oss / NoMADLogin-AD · GitLab. [online]. Dostupné z: https://gitlab.com/orchardandgrove-oss/NoMADLogin-AD/-/wikis/Configuration/preferences
19. GitHub - munki/munki: Managed software installation for macOS —. GitHub: Where the world builds software · GitHub [online]. [cit. 25.8.2021]. Dostupné z: https://github.com/munki/munki
20. Home · munki/munki Wiki · GitHub. GitHub: Where the world builds software · GitHub [online]. [cit. 25.8.2021]. Dostupné z: https://github.com/munki/munki/wiki/
21. Overview · munki/munki Wiki · GitHub. GitHub: Where the world builds software · GitHub [online]. [cit. 26.8.2021]. Dostupné z: https://github.com/munki/munki/wiki/Overview

22. GitHub - hjuutilainen/munkiadmin: macOS app for managing Munki repositories. GitHub: Where the world builds software · GitHub [online]. [cit. 1.9.2021]. Dostupné z: https://github.com/hjuutilainen/munkiadmin
23. GitHub - autopkg/autopkg: Automating packaging and software distribution on macOS. GitHub: Where the world builds software · GitHub [online]. [cit. 2.10.2021]. Dostupné z: https://github.com/autopkg/autopkg
24. GitHub - lindegroup/autopkgr: AutoPkgr is a free Mac app that makes it easy to install and configure AutoPkg.. GitHub: Where the world builds software · GitHub [online]. [cit. 5.10.2021]. Dostupné z: https://github.com/lindegroup/autopkgr#features
25. Master Data Management (MDM) Solutions Reviews 2021 | Gartner Peer Insights. 301 Moved Permanently [online]. [cit. 10.11.2021]. Dostupné z: https://www.gartner.com/reviews/market/master-data-management-solutions
26. Parallels Device Management: Unified endpoint to provide PC, iPad, iPhone and Mac Management. Parallels: Mac & Windows Virtualization, Remote Application Server, Mac Management Solutions [online]. [cit. 30.10.2021]. Dostupné z: https://www.parallels.com/products/device-management/
27. Manage Software Center – obrázek [online]. [cit. 28.11.2021]. Dostupné z: https://raw.githubusercontent.com/wiki/munki/munki/images/managed_software_center.png
28. Vizualizace MDM a služeb pro hromadnou správu zařízení – Obrázek. Apple Help Library [online]. [cit. 28.11.2021]. Dostupné z: https://help.apple.com/assets/5FD2AF22680CE26347806074/5FD2AF24680CE26347806082/cs_CZ/905bbd3ba55dc51197b0676dd5d8b2af.png