Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Analýza a návrh využití CentOS 7 pro adresářové služby v heterogenních sítích

Diplomová práce

Autor: Bc. Tomáš Růžička
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové Duben 2019

Prohlášení:

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

……..

V Hradci Králové, dne Tomáš Růžička

Poděkování:

Touto cestou bych rád poděkoval svému vedoucímu, Mgr. Josefu Horálkovi, Ph.D., který mi vždy pomohl, vyšel vstříc a za vedení již druhé závěrečné práce.

Anotace

Diplomová práce si bere za cíl ověřit možnosti využití adresářových služeb Active Directory na operačním systému CentOS 7 se softwarem Samba verze 4. První část popisuje klíčové pojmy ze zmíněné oblasti a k jejich pochopení je výklad doplněn o schématická znázornění. Uživatel získá přehled o tom, k čemu AD slouží, jaké jsou jeho základní části a jak spolu fungují.

Druhá část za zabývá praktickou konfigurací adresářových služeb, a to včetně úvodního nastavení systému i následné instalaci a ladění Samby. I když je celé nasazení psáno jako sled postupných kroků, předpokládá se ze strany čtenáře alespoň základní znalost platformy GNU/Linux, dále jen Linux. V průběhu práce se uživatel může setkat s mnoha drobnými i velkými problémy, kdy jejich řešení může být pro nezkušeného správce značnou překážkou. Dva takové případy jsou popsány na závěr praktické části.

Annotation

Analysis and design of use of CentOS 7 for Active Directory services in heterogeneous networks

The diploma thesis aims at verifying the possibilities of using Active Directory directory services on the CentOS 7 operating system with Samba version 4. The first part deals with key concepts from the mentioned area and their interpretation is supplemented by schematic illustrations. The user gets an overview of what AD serves, what its essential parts are and how they work together.

The second part deals with the practical configuration of directory services, including the initial setup of the system and the subsequent installation and tuning of Samba. Although the deployment is written as a sequence of step-by-step steps, the reader is expected to have at least basic knowledge of the GNU / Linux platform, Linux. During the setup, the user may encounter many minor and major problems, and their solution may be a significant obstacle for an inexperienced administrator. Two such cases are described at the end of the practical part.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V moderním světě představují informační a komunikační technologie základ téměř každé firmy ať už o pár uživatelích či stovkách a tisících zaměstnanců. S jejich rostoucím počtem se zvyšují nároky na údržby interních systémů a časem vzniká potřeba po vytvoření centrální databáze uživatelů a informací o nich společně s distribucí pravidel (skupinových zásad) pro jednotlivé počítače/uživatele. To správcům umožní efektivnější správu a firma získá udržitelný rozvoj do budoucna.

V této oblasti má dominantní postavení produkt Active Directory provozovaný na Windows Server od společnosti Microsoft. Jedná se o distribuované adresářové služby, které umožňují řízení účtů a počítačů s operačním systémem Windows a nabízí možnost systematického uchování informací o uživatelích a zařízeních ve firemním prostředí.

Windows Server staví na mnoha standardech jako je Kerberos, LDAP nebo SMB. Toho samozřejmě využívají open-source aplikace, který implementují svobodné standardy a tím poskytují spoustu jednotlivých úkonů. Software Samba 4 všechny tyto funkcionality zastřešuje a nabízí komplexní řešení adresářových služeb na platformě Linux.

Samba má za sebou dlouhou historii. Minulé verze se využívaly především pro sdílení souborů, které samozřejmě poskytuje i v doménovém prostředí. Pouze je k němu přidána další funkcionalita. Nové vydání přímo vybízí k integraci do heterogenních sítí s operačním systémem Microsoft Windows a Linux. Samba tedy postupně přibírá funkcionality z AD a nabízí je v open–source variantě, což je pro mnoho firem velice zajímavým argumentem. Stinnou stránkou řešení je právě open-source, a tedy spolehnutí se na komunitu v případě problémů.

2 Cíl práce

Cílem této práce je zjistit možnosti využití CentOS 7 se softwarem Samba 4 jako základu pro Active Directory ve formě open-source.

První část popisuje teoretickou stránku provozu adresářových služeb, vysvětlení jejich základních principů a funkcionalit. Dále je zde zmíněná jejich problematika v kontextu korporátního prostředí a analýza CentOS 7 jako serverového operačního systému. Po teoretickém úvodu je popsána potřebná konfigurace pro provoz doménových řadičů, sdílení souborů a připojení klientů do nově vzniklého prostředí.

Hlavní myšlenkou a cílem je ověřit, zda je alternativní řešení na dostatečné úrovni pro využití v reálném provozu. Práce popisuje i některé případné nedostatky a problémy, které se v jejím průběhu objevily. Nasazení v korporátní sféře by mělo předcházet důkladné testování. Čtenář díky této práci získá přehled o problematice.

3 Literární rešerše

Možnost využití CentOS 7 jako základního systému pro Active Directory (AD) je poměrně specifickou záležitostí, a proto není mnoho odborných publikací zabývající se touto tématikou. Active Directory znamenají adresářové služby zaštítěné společností Microsoft, které jsou provozovány na platformě Windows Server. Jedná se o nástroje, které udržují informace ve formě objektů. Tím mohou být chápány například tiskárny či samotní uživatelé. Ačkoli existuje pár alternativ založených na Linuxovém základu, Microsoft je v této oblasti stále vůdčím hráčem.

Ovšem i přes jeho významné postavení není nutné se omezit pouze na sítě složené z Windows stanic a serverů. Jelikož tato technologie staví na otevřených standardech, tak se přímo nabízí zapojení do heterogenního prostředí složeného z platformy Windows od společnosti Microsoft, OS X (či nově Mac OS) pod křídly Apple Inc. nebo systémy založené na platformě Linux. O možnostech využití platformy Mac OS X jako systému pro provoz adresářových služeb a jeho nastavení se zabývá kniha Enterprise Mac Administrator's Guide. Autoři zde popisují, co dané služby znamenají, k čemu slouží, jak je nastavit a také jakým způsobem propojit tuto technologii s AD. To umožňuje přiblížit světy uživatelů Windows a Mac. (Smith, a další, 2015)

Klíčovou roli pro tuto práci hraje Linux. Jedná se o svobodný operační systém, kde lze využívat produkty i zcela zdarma (výjimku může tvořit například zpoplatněná prioritní podpora) a v mnoha alternativách. Myšlenka svobodného softwaru se líbila autorovi knihy Pro Freeware and Open Source Solutions for Business (Whitt, 2015). Jako majitel menší firmy ocenil možnost snížení finančních nároků na mnoho produktů potřebných k řízení firmy. Ať už se jedná o tradiční nástroje jako jsou MS Office (LibreOffice dokumenty, tabulky, prezentace), Photoshop (GIMP) či antivirové řešení Windows Defender (Avira). Přitom se nemusí jednat pouze o jednotlivé aplikace. V Linuxu existují alternativy pro celé služby ve formě distribucí, jak je ukázáno v publikaci Introducing Linux Distros (Jose, 2016). Lze tedy využít i jiné řešení než Windows Server, například pomocí Zentyal Server nebo Univention Corporate Server.

Zentyal je komplexní aplikací založenou na distribuci Linuxu zvané Ubuntu. O jeho možnostech a nastavení se lze dočíst v oficiální dokumentaci (Zentyal S.L., ©2017). V ní je popsána instalace v roli primárního řadiče domény, případně jeho

zálohy a dalších podstatných služeb. Následně ho lze provozovat jako alternativu Windows Server s AD modulem.

Stejně jako Zentyal i Univention Corporate Server umožňuje provozování doménového serveru. Všechny podrobnosti se lze dočíst na oficiální webové stránce s dokumentací (Univention GmbH, ©2017). Samotný systém běží na Debian základu a opět umožňuje propojení s Microsoft řešením.

Obě možnosti mají své výhody i nevýhody a snaží se co nejvíce napodobit fungování AD či obecněji Windows Serveru, ale na zcela jiné platformě. To s sebou přináší svá omezení, ačkoli technologie staví na definovaných standardech.

V této práci bude využita kombinace systému CentOS 7 a nástroje Samba. Pro ně je tedy potřeba představit hlavní zdroje informací. Jedním z nich je System administrator's guide spravovaný Marií Doležalovou a kolektivem z rodičovského operačního systému RHEL společnost Red Hat, inc. (Red Hat, Inc., ©2017). CentOS je jeho přímý derivát udržovaný komunitou (The CentOS Project, ©2017). Popisuje celý operační systém a představuje ucelenou příručku každého administrátora nejen RHEL.

Implementací Samby, ale na starší systém Debian 7, se zabývá kniha Implementing Samba 4 od Marcelo Leal. Autor v ní popisuje potřebnou konfiguraci, ale z dlouhodobého hlediska je využití starého systému neperspektivní. (Leal, 2014)

Klíčová je dokumentace zmíněného softwaru, který je použit pro AD na CentOS 7. Ta je dostupná na adrese wiki.samba.org a administrátor si zde může přečíst veškeré možnosti a nastavení daného softwaru.

4 Principy a funkcionality Active Directory

Active Directory je jedna z klíčových vlastností Windows Server již od verze 2000. Představuje soubor informací (adresář) o každém uživateli, počítači, tiskárně nebo nastavení. Všechny informace jsou uloženy v logických strukturách a ty mají mezi sebou určitě vztahy (tvoří hierarchickou strukturu). AD představuje centrální způsob uložení a řízení informací ve formě objektů (organizační jednotky, z angl. „organizational units“), které je možné spravovat na jednom místě. Jedná se o proprietární implementaci adresářových služeb firmou Microsoft. (Hannifin, a další, 2010 stránky 141-156)

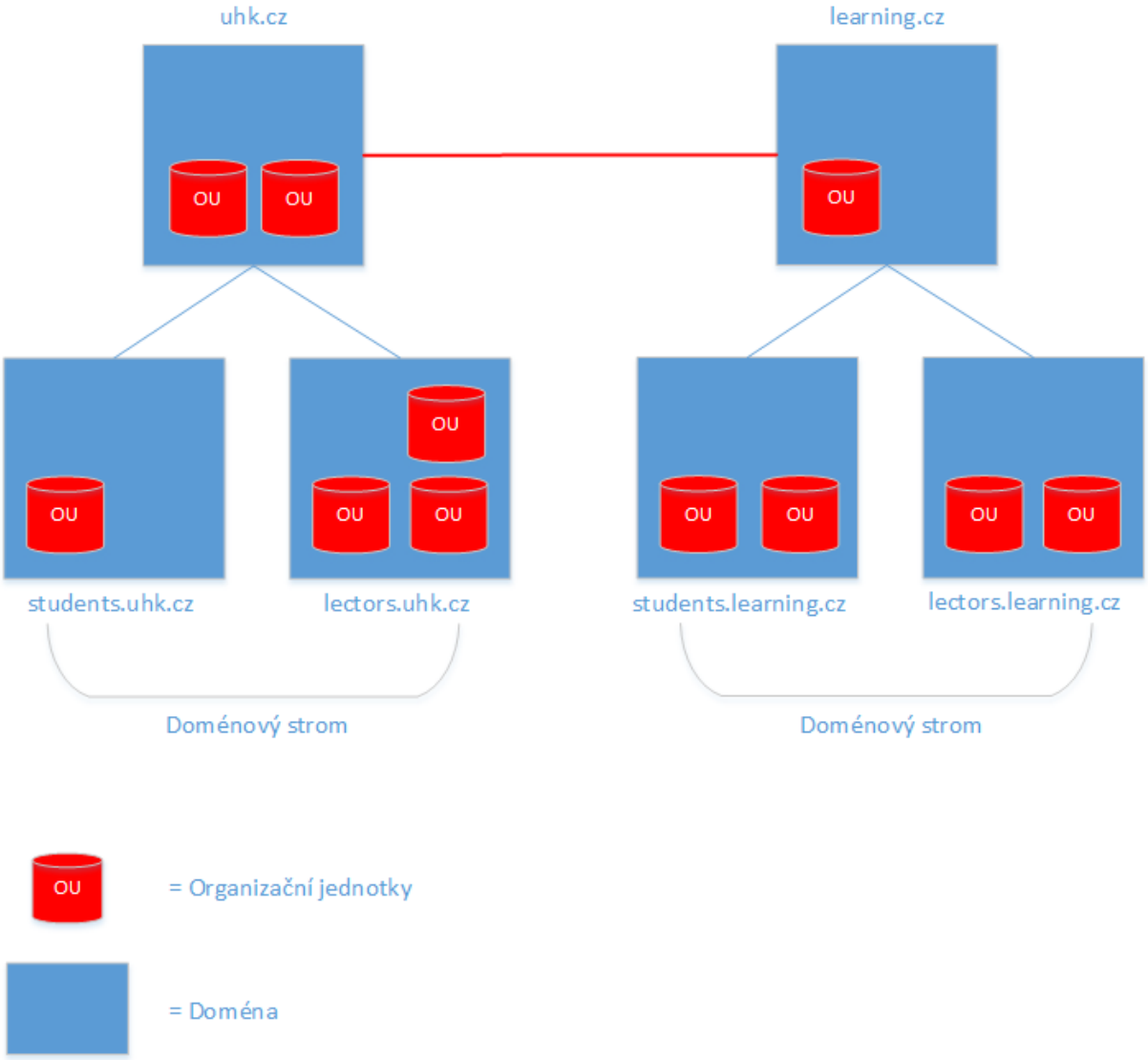
Smyslem systému je umožnit jednoduchou správu objektů, globální bezpečností politiky a všech pravidel správcům systému. Ti jsou schopni pomocí dodaných nástrojů konfigurovat příslušná nastavení a publikovat je v rámci firemního prostředí. Výsledné řešení přináší i vyšší komfort pro uživatele, kteří se mohou přihlásit pod svým účtem do domény a využít předdefinované nastavení, které je aplikovatelné na libovolný počítač. Celý mechanismus je řízen pomocí jednoho či více doménových řadičů, takže systém dokáže pracovat v režimu vysoké dostupnosti a být tak chráněný pro případ poruchy.

4.1 Struktura

AD se skládá z několika druhů komponent, přičemž celkově tvoří hierarchickou strukturu. Ta je silně provázána s DNS a bez něj by služba nemohla fungovat. DNS (angl. „Domain Name System“) je systém, který převádí snadno zapamatovatelná jména na IP adresy a ty se dále používají pro komunikaci.

Mít celou organizaci v jedné struktuře by bylo s rostoucí velikostí neefektivní. Proto se zde využívá stejného principu jako u DNS a celek se rozpadá na jednotlivé logické subsystémy (nejčastěji stromy a domény).

Logické schéma může vypadat následovně (Obrázek 1, str. 6).



Obrázek 1 - Příklad logické struktury Active Directory

V obrázku (Obrázek 1) je naznačena možná struktura použití. Mezi základní jednotky patří: (Microsoft Corporation, ©2014a)

- Les
- Strom
- Doména
- Organizační jednotka

4.1.1 Les

Les je nejvyšší jednotka nad všemi doménami, které patří k dané instanci AD. Obsahuje jeden či více stromových struktur, jež se dále rozpadají na menší části. Jako celek tvoří bezpečností hranici pro vytvořený systém.

4.1.2 Strom

Les se skládá ze stromů a ten je složen z jedné či více domén. Při přidání další domény do stromu se stává potomkem rodičovské domény dané oblasti, a to včetně jména z DNS (sdílí společný prostor). Pokud je strom složený z uhk.cz, tak může mít přímé potomky students.uhk.cz, lectors.uhk.cz nebo i top.students.uhk.cz.

Pokud správce přidá další doménu, která nesdílí stejný jmenný prostor, stává se automaticky kořenovou doménou v nově vzniklém stromu.

Domény v rámci stromu obsahují oboustrannou tranzitivní důvěru. To znamená, že když students.uhk.cz má důvěru s lectors.uhk.cz a lectors.uhk.cz má důvěru s external.uhk.cz, tak i students.uhk.cz má důvěru s external.uhk.cz. V praxi to lze využít tak, že students.uhk.cz přijímá ověřování vůči external.uhk.cz.

4.1.3 Doména

Doména již obsahuje jednotlivé položky z kategorie organizační jednotky (jedná se o hranici pro danou instanci). V rámci ní je nastavena bezpečností politika, přístupová práva (ACL) a sdílí společnou databázi. Všechna nastavení nepřekračují hranice tvořené danou doménou.

4.1.4 Organizační jednotky

Tvoří základní prvky celého systému. Existuje mnoho druhů, například uživatelé, skupiny, tiskárny či sdílené složky. Objekty s podobným nastavením lze shlukovat do dalších organizačních jednotek, takže pravidla lze aplikovat na nejvyšší úrovni a ta jsou automaticky přenesena na potomky.

4.2 Doménový řadič

Tato kapitola čerpá ze zdroje (Stanek, 2009 stránky 26-29) a (Microsoft Corporation, ©2018c stránky 321-322).

Všechny domény mají svůj doménový řadič (DC), který obsahuje příslušný adresář služby AD. Ten má za úkol chránit veškeré informace o objektech, řídit jejich aktualizace, spravovat přihlašování a poskytovat další důležité služby.

Uchovávat nastavení na jednom místě přináší administrátorský komfort oproti lokální konfiguraci na každém počítači. Veškeré změny by se musely ručně upravovat na všech koncových zařízeních. Myšlenka centrálního uložiště zefektivňuje celý proces, ale zároveň představuje problém. SPOF (ang. „Single point of failure“ neboli koncept selhání jednoho systému a následného zastavení celého firemního procesu), který lze v prostředí Windows Server jednoduše vyřešit více doménovými řadiči. Ty si mezi sebou replikují data a selhání jednoho neohrozí fungování zbytku firmy. Standardně mají servery právo ke čtení i zápisu, ale například pro odlehlejší řadiče je možné definovat právo pouze pro čtení RODC (angl. „Read only domain controller“). Tyto instalace poté nemohou replikovat data na zbytek serverů, ale pouze stahovat změny k sobě, a ohrozit tím bezpečnost zbytku domény.

4.3 DNS

Tato kapitola čerpá ze zdroje (Stanek, 2009 stránky 24-26).

Nezbytnou součástí pro fungování systému je služba DNS. Její úkol je překládat jména zařízení na IP adresy a rozděluje celý ekosystém do mnoha domén. Počítače v rámci domény sdílí stejný jmenný prostor a jejich nadřazený DNS server se stará o správný překlad adres. Pokud se jedná o zařízení mimo spravovaný celek, předá DNS server požadavek na svůj nadřazený DNS serveru a tímto způsobem se systém dotazuje, dokud nezíská správný (či chybějící) výsledek.

V praxi se doménový název skládá z více jmen. Základní jednotkou jsou tzv. domény nejvyššího řádu (například cz, de či com nebo org). Další názvy oddělené tečkou se označují jako subdomény, které se hierarchicky třídí. Například tiskárna s číslem 22 patřící firmě Company (s doménou company.com) na její pobočce v Praze pro obchodní oddělení může mít název: printer22.sells.prague.company.com.

V rámci Active Directory je nutné mít funkční systém DNS, případně je možné při instalaci Windows server aktivovat průvodce pro jeho doinstalování. Bez něj služba nebude fungovat.

4.4 Důvěra

Tato kapitola čerpá ze zdroje (Microsoft Corporation, ©2009) a (Microsoft Corporation, ©2012).

Důvěra v rámci AD je princip, kterým se ověřuje požadavek mezi doménami. Pokud chce uživatel z jedné domény přistoupit do jiné, kontaktuje svůj řadič a může získat důvěru pro přístup do dané oblasti. Ta byla dříve pouze jednostranná a netransitivní. Od verze NT 5.0 (Windows 2000) můžou být vztahy oboustranné a transitivní. Pro připomenutí, transitivní vztah znamená, že když students.uhk.cz má důvěru s lectors.uhk.cz a lectors.uhk.cz má důvěru s external.uhk.cz, tak u students.uhk.cz má důvěru s external.uhk.cz. Zmíněné funkčnosti lze využít pro zvýšení zabezpečení tím, že z domény A lze kontaktovat B, ale opačně tento postup není možný. Pokud by došlo ke kompromitování sítě B, tak AD lokality A je chráněno touto jednostrannou důvěrou. Důvěra samozřejmě nezabrání jinému napadení, ale na úrovni Active Directory je útok minimalizován.

Uživatel požadující přístup do jiné domény v rámci stejného lesa kontaktuje svůj doménový řadič, který zajistí ticket pro přístup k externím zdrojům na dané doméně a vrátí ho uživateli. Ten ho následně využije pro přímý dotaz na požadovanou doménu a ověří se získaným tiketem.

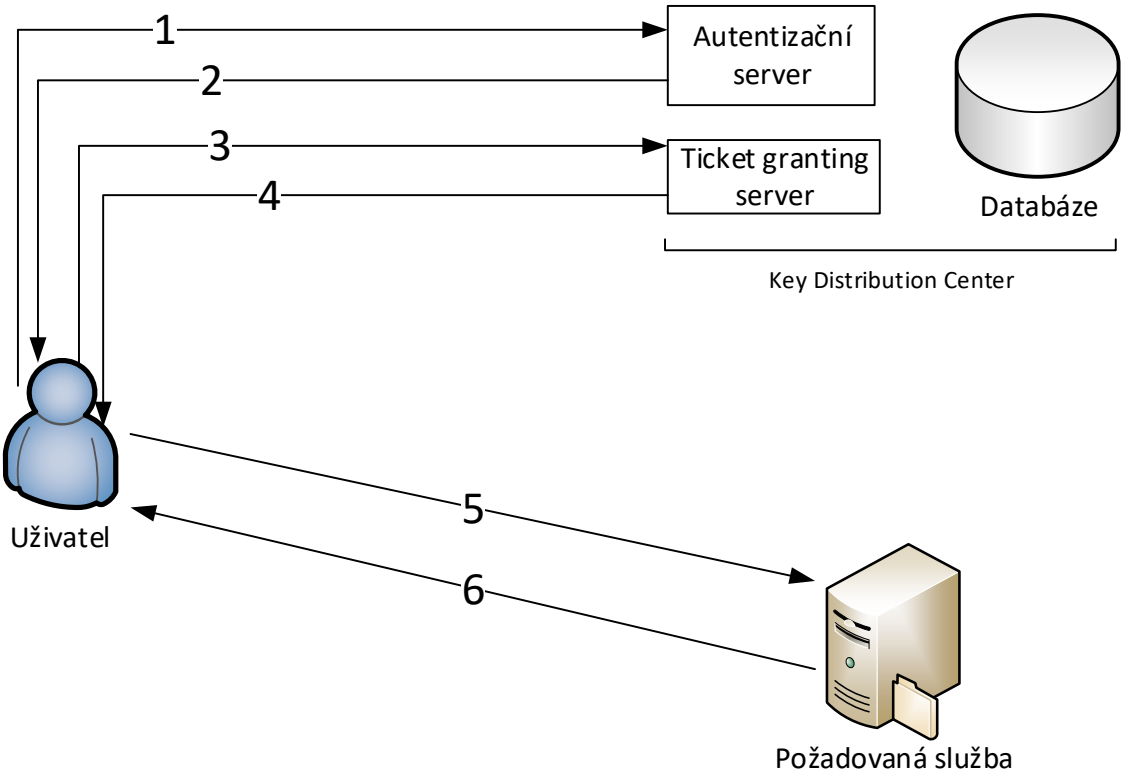
4.4.1 Kerberos

Tato kapitola čerpá ze zdroje (Ricciardi, 2007) a (Microsoft Corporation, ©2012)

Aby bylo možné vytvářet vztahy důvěry, je nutné zajistit proces autentizace, tedy ověření. K tomu se v prostředí Windows využívá dvou protokolů – NTLM a Kerberos. Kerberos je nástupcem již zastaralého NTLM, a proto bude podrobněji popsán pouze on.

Ve své podstatě je Kerberos autentizační (jednoznačné určení uživatele) protokol, který využívá principu sdílených klíčů a symetrického šifrování (šifrování i

dešifrování pomocí stejného hesla). Původně byl vyvinut na MIT (Massachusetts Institute of Technology). Svůj název dostal podle mýtického stvoření, psa Kerbera, který střežil vstup po podsvětí a měl tři hlavy. Stejně tak v IT prostředí chrání přístup k jednotlivým službám. Jeho myšlenka je umožnit bezpečné ověření uživatele v nezabezpečeném prostředí. Pokud se na něj nahlíží jako na komplexní nástroj v systému, pak ho lze považovat i za autorizační (ověření, zda má přístupová práva), jelikož se podílí na celém procesu. Nicméně pravidla přístupu jako taková se řídí konkrétním nastavením pro danou organizaci, respektive uživateli v AD. Základní schéma komunikace v protokolu je následující.



Obrázek 2 - Princip komunikace uživatele s KDC a požadovanou službou. Převzato a upraveno z: (Ricciardi, 2007)

Srdce implementace se nazývá KDC (angl. „Key Distribution Center“), které se skládá ze třech součástí. Autentizačního serveru (AS), Ticket granting serveru (TGS) a databáze. AS ověří, že uživatel je skutečně ten, za koho se vydává a TGS dává ověřenému uživateli klíč k požadované službě. Pro celý systém je nesmírně důležité správně nastavený čas na serverech i jednotlivých zařízeních. Tomu bude kladem důraz i v praktické části. Některé požadavky obsahují značky a dobu, po kterou je

možné daný autentizační proces provést. Pokud by čas rozcházel mezi uživatelem a serverem, nebylo by možné projít všemi potřebnými kroky a akce by selhala. K tomuto účelu lze využít pomocného protokolu NTP, který zajistí správnou synchronizaci času na všech zařízeních s minimální odchylkou.

V prvním kroku (`AS_REQ`) uživatel pošle zcela nešifrovanou zprávu (angl. „plaintext“) autentizačnímu serveru se svým jménem, typem požadované služby (což je nyní služba TGS), IP adresami s oblastí, kde chce tiket použít a maximální dobu pro vyřízení.

Následně server ověří, zda uživatel a služba existuje a pošle zpět dvě zprávy (`AS_REP`). První část obsahuje zkopírované údaje z `AS_REQ`, tedy uživatele, službu (TGS) a IP adresy. Také je zde časové razítko, validita požadavku a klíč zvaný „TGS session key“. Nyní již dojde k zašifrování zprávy pomocí TGS klíče, ke kterému nemá uživatel přístup. Druhá zpráva obsahuje službu, časové razítko, časovou validitu a „TGS session key“. Celá je zašifrována pomocí klíče daného uživatele. Ten je po přijmutí zprávy vyzván k jeho zadání. Pokud dojde k úspěšnému dešifrování, je uživatel skutečně tím, kým se prohlašuje být a získá „TGS session key“, pro šifrování další zprávy. Pokud se jedná o útočníka, bude mít dvě zašifrované zprávy, které nemůže přečíst. Tímto způsobem je zajištěna autentizace uživatelů bez toho, aniž by bylo nutné posílat hesla v nezabezpečené podobě skrze síť. Není tedy potřeba zabezpečit celý komunikační kanál, jelikož to zvládají zprávy samy o sobě.

V druhé části se uživatel dotáže TGS, aby získal lístek (angl. „ticket“) pro službu, kterou chtěl původně navštívit (například souborový server). Pokud je vše v pořádku, obdrží ticket pro koncovou aplikaci a zašle požadavek přímo na ní bez toho, aniž by se musel dále přihlašovat. Princip se nazývá SSO (jedno přihlášení pro všechny aplikace, z angl. „Single sign-on“). Není potřeba získat uživatelské jméno a heslo pro každou požadovanou aplikaci, ale pouze jednou, a to vůči službě Kerberos. Pro zabezpečení zpráv se lze spolehnout například na ověřenou šifru AES256, která se řadí mezi kvalitní a spolehlivé algoritmy.

4.5 Flexible single-master operations role

Tato kapitola čerpá především ze zdroje (Microsoft Corporation, ©2014b) a (Samba project, ©2017c).

Dřívější implementace AD využívali princip primárního (PDC) a jednoho či více záložních doménových řadičů (BDC). Změny byly směřovány právě na PDC a následně distribuovány na BDC. Nový přístup situaci mění a editaci údajů je možné provádět na všech serverech. Nazývá se multi-master a AD se následně postará o replikaci změn. Technicky se jedná o mnohem náročnější záležitost než jeden centrální systém, který kopíruje změny na záložní. Zde mohou vznikat kolize a tedy problémy. Ty jsou řešeny způsobem, že poslední (nejaktuálnější) změna vyhrává a ostatní jsou zahozeny. Tímto přístupem ale některé operace řešit nelze. Proto i v takovém prostředí je jeden (nebo více) ze serverů důležitější než ty ostatní. Nese tzv. FSMO role.

FSMO (flexible single-master operations) představují kritické součásti systému, které běží na hlavním serveru. (Stanek, 2009 str. 183) Byly zavedeny právě ze zmíněných důvodů multi-master prostředí a připomínají princip PDC/BDC. Několik klíčových úloh je vždy zpracováváno na konkrétním serveru, který nese příslušnou roli a následně je změna replikována do zbytku infrastruktury. Tím je zajištěna integrita, ale částečně se ztrácí výhoda multi-master prostředí.

Dle Microsoft zdroje se mezi FSMO role řadí:

Schema Master (server schémat)

- Řídí změny v adresářovém schématu, které určuje třídy v lese a atributy v objektech.

Domain Naming Master (server názvů domén)

- Dokáže přidávat nebo odebírat domény.

RID Master (server RID)

- Přiděluje relativní ID (RID), které je součástí jednoznačného bezpečnostního identifikátoru (SID) každého objektu.

PDC Emulator (emulátor primárního řadiče domény)

- Poskytuje časové služby počítačům se systémem Windows v doméně.
- Pracuje se změnou hesla, chybným přihlášením a zablokovanými účty.

Infrastructure Master (server infrastruktury)

- Aktualizuje SID – změny členství ve skupinách a DN (identifikátor objektu).

Nicméně dle zdroje (Samba project, ©2017c) a oficiálního článku od společnosti Microsoft (Microsoft Corporation, ©2018d) existují další dva, které nejsou v předešlém odkazu zmíněny. Jedná se o **Domain DNS Zone Master** (server spravující doménové DNS zóny) a **Forest DNS Zone Master** (server spravující DNS záznamy v rámci lesů). Oba mají na starosti editaci DNS zón zapojených do AD, ale na jiné úrovni (domény/lesa).

FSMO role mohou být rozmístěny na různých serverech pro eliminaci rizika selhání systému v případě poruchy a rozložení zátěže. Rozdělení není nutné mít na začátku tvorby AD, ale je možné je rozmístit ve fungujícím prostředí. Stačí vybrat nový server, který bude provádět danou roli a zadat příkaz k přesunu. Nemusí se přitom jednat jen o plánovaný úkon. Při selhání serveru obsahující FSMO roli musí dojít k jeho zastoupení jiným. V té situaci ale nelze přikročit ke standardnímu přesunu, a proto lze provést i násilné převzetí odpovědnosti.

Pochopení a udržování těchto funkcí je klíčové pro správné fungování celého AD. I když se dané změny replikují na další doménové řadiče, je vhodné předcházet výpadku. Pokud dojde k hardwarové poruše, musí administrátor zasáhnout a postarat se o zastoupení jiným serverem s příslušnou konfigurací.

V Linuxovém prostředí s využitím softwaru Samba lze zobrazit FSMO role a jejich rozložení následujícím příkazem.

```
[root@dc1 ~]# samba-tool fsmo show

SchemaMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=company1,DC=local

InfrastructureMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=company1,DC=local

RidAllocationMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=company1,DC=local

PdcEmulationMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=company1,DC=local

DomainNamingMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=company1,DC=local

DomainDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=company1,DC=local

ForestDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=company1,DC=local
```

5 Standardní model nasazení AD v korporátních sítích

Služby Active Directory jsou v IT světě jednoznačně silným nástrojem pro správu středních a velkých podniků. V malých provozovnách o pár zaměstnancích lze veškeré akce a údržbu provádět ručně. Nicméně s jejich rostoucím počtem se stále zvyšuje efektivita nasazeného systému a rozevírají se ekonomické nůžky mezi zakoupením a údržbou systému AD a neautomatizovanou prací ICT pracovníků. Ti díky centrální správě mohou pružně reagovat na aktuální požadavky, mít globální přehled o stavu systému a celý ho řídit.

Nasazením zmíněného produktu firmy řeší několik požadavků, mezi které patří:

- Správa uživatelů a zařízení
- Definice služeb a zdrojů
- Řízení oprávnění, role
- Distribuce nastavení mezi všechna zařízení
- Centrální uložení dat
- SSO
- Audit
- .. a další

5.1 Ochrana dat a služeb

Při rozhodnutí o využití adresářových služeb je nutné myslet na úroveň zabezpečení, kterou lze rozdělit na autonomní a kompletní izolaci. Izolace znamená, že daná skupina má exkluzivní kontrolu nad svými zdroji a není možný externí zásah. Naopak v autonomii je řízení sice nezávislé, ale není izolované. To v důsledku vypadá tak, že vyšší administrátor může spravovat více autonomních jednotek, a přitom může mít každá svého lokálního, který řídí jen své zdroje. Například určitá část organizace může vyžadovat striktně oddělený přístup k datům, a proto využije principu izolace a řídí si vše sama. (Microsoft Corporation, ©2018c stránky 307-309)

5.2 Plánování

Před tím, než dojde k samotnému nasazení je potřeba důkladně promyslet, jak má budoucí systém fungovat. Logická struktura následně určuje, jak bude vypadat

rozložení lesa, domén a samotných organizačních jednotek v rámci společnosti. Následně se k návrhu přidají i fyzické aspekty, jako je propustnost linek mezi servery pro zajištění bezproblémové replikace, počet doménových řadičů či zbytek síťové topologie. (Microsoft Corporation, ©2018c stránky 281-282)

V rámci tvorby lesa je potřeba vyřešit, jak má být společnost rozdělena. Jeden les obsahuje stejné schéma pro všechny domény v něm obsažené (schéma definuje typy objektů a jejich možné informace). Pokud je toto potřeba rozlišit, jen nutné použít další les. Dalším příkladem mohou být právní požadavky, které nutí striktně oddělit určité informace či použít jiné metody. V neposlední řadě je potřeba si uvědomit, že správce lesa má přístup ke všem datům uloženým v jeho hierarchické struktuře. Jejich oddělením se podstatě zvýší bezpečnost a sníží riziko chybného nastavení či útoku škodlivého softwaru. (Microsoft Corporation, ©2018c stránky 302-306)

Při nasazení více lesů přichází na řadu vztah důvěry. Ten určí, jestli se jedná o zcela oddělené jednotky, vzájemně spolupracující nebo jednostranně využívající. Poslední možnost lze aplikovat na případ, kdy určitá část společnosti má své zdroje, zároveň využívá přístupu do centrální oblasti, ale v případě problémů v této části musí být provoz zachován a zvládne fungovat zcela samostatně. Naopak centrální jednotka nemůže do této části zasáhnout, a tudíž ji ani ohrozit. (Microsoft Corporation, ©2018c stránky 310-314)

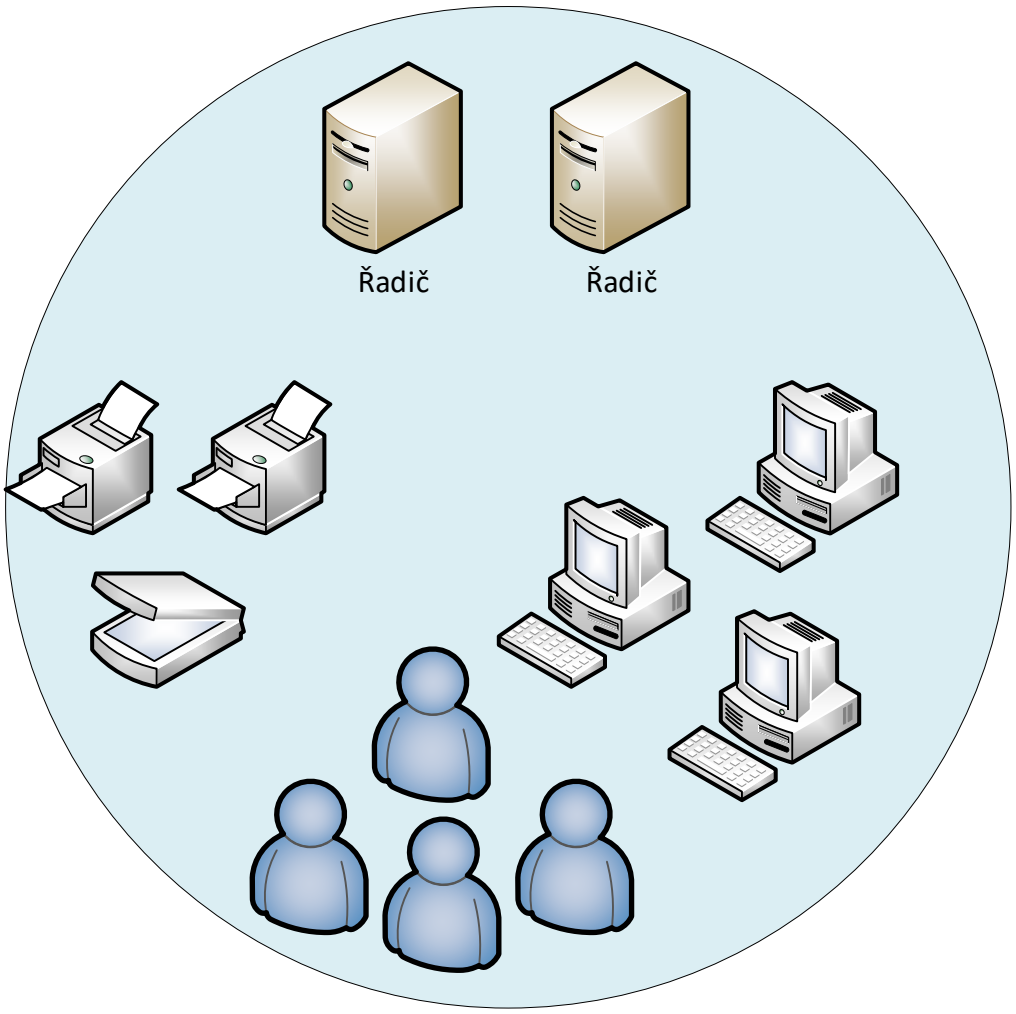
Po dokončení návrhu lesů dojde na samotné domény. Ty dělí organizaci do menších částí a na rozdíl od vyšších jednotek zde nelze aplikovat princip izolace zdrojů. Při vytváření jednotlivých domén je potřeba vzít v úvahu počet uživatelů a rychlost linky. Doména může obsahovat více řadičů, jež mezi sebou replikují data, která při velkém počtu a nízké propustnosti mohou způsobovat problémy. Použití jedné domény je jednoduché z hlediska komplexnosti systému, ale při vysokém počtu uživatelů je vhodné je rozdělit do více regionálních domén. Následně mohou řadiče v rámci domény replikovat méně dat a tím nezatěžovat linku. To stejné platí například pro pomalé spoje na dlouhou vzdálenost. Nicméně použití více doménových řadičů je nutností pro zavedení HA (vysoká dostupnost, z angl. „high availability“). Pokud by byl k dispozici pouze jeden, nebudou služby AD po výpadku k dispozici. (Microsoft Corporation, ©2018c stránky 321-325)

Jelikož servery pracují v režimu vysoké dostupnosti, může změna na jednom z nich ohrozit bezpečnost všech ostatních. Proto je možné využít RODC (řadiče pouze pro čtení), které replikují data jen na sebe, ale již neposílají změny provedené na nich do zbytku domény. Tím lze provést změny na RODC a nechat je pouze na něm. (Microsoft Corporation, ©2018c str. 322)

V prostředí kde je více domén je důležité vhodné umístění dostatečného množství globálních katalogů. Ty slouží ke shromažďování částečných informací o všech objektech ve všech doménách v rámci v lesa. Například pokud je požadováno přihlášení uživatele v multidoménovém prostředí, je kontaktován globální katalog, který má potřebné informace. Dalším požadavkem může být vyhledání tiskáren. Bez globálního katalogu by bylo potřeba kontaktovat všechny domény a jejich řadiče. S ním jsou tyto informace umístěny na jednom místě (případně na replikách) a server může rychle odpovědět na globální dotaz. (Stanek, 2009 stránky 155-157)

Po rozdělení domén se pozornost přesouvá na samotné OU. Ty definují veškeré typy jednotek a uživatelů v AD, kterých může být v rámci organizace klidně desetitisíce. Špatným návrh systému může vést k přetížení určitých částí a zmíněných problémů s replikací. (Microsoft Corporation, ©2018c stránky 321-325)

Vyřešením logické struktury a síťové topologie se může přejít do fáze instalace systému. Zde je vhodné zmínit způsob licencování AD. Pro jeho provoz jsou potřeba samotné licence Windows Server jako takového, ale následně i tzv. CAL licence. Na rozdíl od Windows Serveru, který se týká samotných serverů (jejich instalací), tak CAL jsou určeny na uživatele/zařízení používající systém v rámci společnosti. (Hannifin, a další, 2010 stránky 11-12)



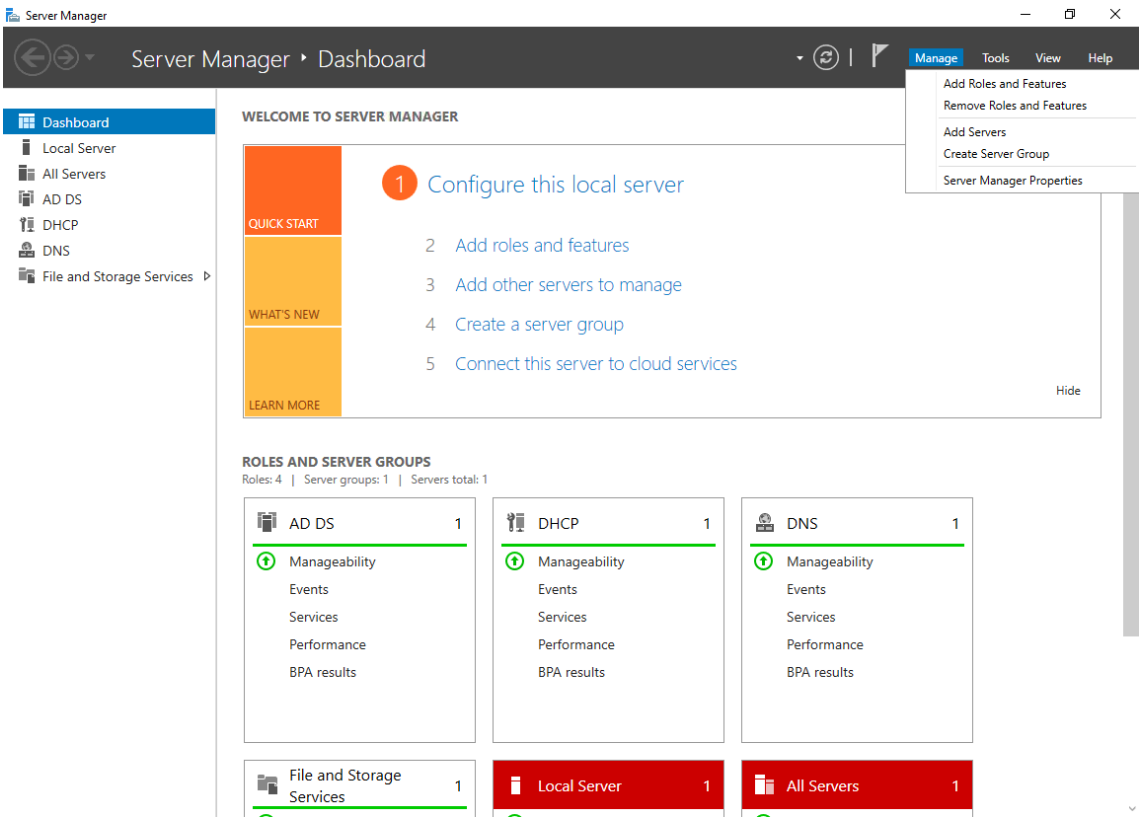
Obrázek 3 - Příklad domény v AD

5.3 Nasazení

Po pečlivě připraveném návrhu řešení a nákupu licencí je možné přejít do fáze realizace. Nicméně tato diplomová práce se primárně zabírá nasazením adresářových služeb na alternativní platformě. Konkrétně za pomoci Linuxové distribuce CentOS 7 a softwaru Samba. Proto budou vybrány jen určité části konfigurační fáze.

Začátek instalace systému probíhá stejným způsobem, jako jsou uživatelé zvyklí z Windows 10. Správce si volí z edic Essentials, Standard a Datacenter. První z nich je určena pro malé podniky o pár uživatelích (nejsou potřeba CAL licence). Standard je klasická plná verze Windows Server pro podniky, kde se počet uživatelů a zařízení určuje pomocí zmíněných CAL. Třetí je přímo pro datacentra. (Microsoft Corporation, ©2018b)

Po úspěšném nainstalování základního systému má administrátor k dispozici propracované grafické rozhraní zvané Server Manager, skrze které má rychlý přehled o stavu systému a všech služeb, včetně konfigurace. Jedná se o lokální nástroj. Správce musí být lokálně přihlášen nebo mít vzdálenou plochu.



Obrázek 4 - Server Manager ve Windows Server 2016

Bohužel tento nástroj nebude k dispozici v průběhu nasazení AD na CentOS. Jedná se čistě o proprietární software společnosti Microsoft. Místo toho se využijí tzv. RSAT (nástroje pro vzdálenou správu, z angl. „Remote Server Administration Tools“). Ty jsou kompatibilní s Windows Server 2016 i softwarem Samba a jak již název říká, jedná se o nástroje, díky který lze konfigurovat systém i bez fyzického přístupu či vzdálené plochy. (Microsoft Corporation, ©2017a)

Pro instalaci AD stačí v Server Manageru zvolit volbu `Add roles and features` a proklikat se na výběr služeb. V seznamu objeví `Active Directory Domain Services`. Po zaškrtnutí si systém automaticky zkontroluje potřebné závislosti, a pokud nejsou nainstalované, nabídne je ihned uživateli k doinstalování. V tomto kroku není nutné vybírat i volbu `DNS Server`, nicméně jak bylo zmíněno

dříve, je nutné mít funkční DNS v rámci organizace pro fungování AD. Pokud není k dispozici, může se využít (doinstalovat) ten ve Windows Serveru pouhým zaškrtnutím další služby.

Nyní si systém nainstaluje adresářové služby a je možné z něj udělat doménový řadič pouhým kliknutím na `Promote this server to a domain controller`. Pokavaď v síti není již funkční prostředí, vytvoří se za pomoci průvodce nový les a doména. V opačném případě lze server připojit do již existující struktury.

Důležitá je volba `Functional level`, jež určuje množinu funkcí dle vydaných verzí Windows Serveru, které budou k dispozici na úrovni domény/lesa. Samba se v současné době řadí na úroveň poskytovanou Windows Server 2008 R2, přičemž částečně má implementované i vlastnosti z verze 2012 a 2012 R2. (Samba project, ©2017e)

Po dokončení instalace a restartu serveru jsou v rámci Server Manager k dispozici nástroje pro správu uživatelů, počítačů, domén a dalších.

Nasazení Active Directory na Windows Serveru 2016 je poměrně snadnou záležitostí pro správce, a to především díky propracovanému grafickému rozhraní a jednoduché konfiguraci. Instalátor vyřeší všechny potřebné závislosti, zjistí od uživatele pár potřebných hodnot a podle nich vše nakonfiguruje.

Oproti tomu instalace na CentOS probíhá v konzoli, která je velice typická pro Linuxový svět. To je v prostředí Microsoft taky možné, ale pouze u verze Core, která tvoří minimalistickou instalaci.

5.4 Rozšířená konfigurace – manažer identit

Velké společnosti obvykle mívají mnoho informačních systémů (dále jen IS), které spolu mohou a nemusí komunikovat. Každý z nich má na starosti určitý úsek práce a v lepším případě mají mezi sebou propojení. Uživatelé pak využívají výhod sdíleného prostředí, jako je omezení duplicity dat z důvodu centrální správy, SSO či snadného přenosu informací. Systémy si navíc musí důvěřovat, což v případě AD představuje vztah důvěry mezi doménovými řadiči.

Na druhou stranu, pokud spolu systémy nespolupracují, musí si pracovníci postupně zřizovat účet do jednotlivých systémů. Jedná se o technicky jednoduché řešení, které nevyžaduje propojení IS, ale případná změna informací o daném uživateli

není automaticky distribuována napříč všemi systémy. Uživatel, případně jiná osoba (správce), musí změnit své údaje ve všech systémech, což je náchylné k chybě. Například pokud by firma ukončila pracovní poměr se zaměstnancem a ten nesdělil všem správcům nový stav, nemusí dojít k odstavení účtů daného uživatele a tím vzniká bezpečností riziko a nekonzistence dat napříč IS. Daná osoba mohla zatajit zrušení VPN účtu pro vzdálený přístup k firemním datům a odejít ke konkurenci. Řešení problému může být IdM (správa identit, z angl. „identity management“).

IdM je celý proces životního cyklu pracovníků společnosti, přičemž zahrnuje správu identit, oprávnění přístupu ke zdrojům, řízení toku informací. Jednotlivé systémy jsou připojeny do vhodného manažeru, kde jsou definována pravidla pro přidělení zdrojů. Odchod zaměstnance potom vypadá jinak. Pracovník na oddělení lidských zdrojů zadá změnu statusu uživatele, manažer identit ji vyhodnotí a odebere dané identitě přiřazené role. Díky tomu všechny systémy reflektují příslušnou změnu, jelikož uživatel nově nemá oprávnění k přístupu.

Z pohledu AD nemají dané doménové řadiče mezi sebou vztah důvěry, ale dotazy na oprávnění ke zdrojům probíhají přes připojený manažer identit. Ten předá požadované informace a řadič je vyhodnotí. To s sebou přináší nejen zvýšení bezpečnosti, ale také nezávislost. Část řadičů může být na platformě Windows Server, jiná na Linuxu nebo iOS. Všechny poté komunikují s centrálním serverem pro identity a není nutné řešit kompatibilitu mezi jednotlivými servery AD.

6 Analýza možností využití CentOS jako AD

Microsoft je se svým proprietární řešením adresářových služeb lídrem v této oblasti. Active Directory se používá od malých podniků až po celosvětové korporáty a to nejen díky svému přívětivému grafické rozhraní zmíněnému v předchozí kapitole. V produktovém listu se lze dočíst, že Windows Server 2016 Standard edice dokáže pojmout až 16 777 216 připojení pomocí SMB protokolu (sdílení souborů) (Microsoft Corporation, ©2017b). V tomto případě může být pro běžné použití limitujícím faktorem spíše cenová politika. S nutností zakoupit nejenom Windows Server, ale hlavně CAL licence pro každého uživatele/zařízení se z výborného pomocníka stává poměrně nákladná položka. Proto mnoho firem a nadšenců hledá alternativní řešení. To tu naštěstí je a jmenuje se Samba a Linuxové distribuce.

Pro účely této diplomové práce bude základní kámen tvořit CentOS ve verzi 7.5. V současné době se jedná o nejnovější vydání tohoto systému založené na placené distribuci RHEL (Red Hat Enterprise Linux) od společnosti Red Hat. Pokud firma hledá alternativu vůči Microsoft řešení, případně potřebuje provozovat některý software na Linuxu, je RHEL zajímavou volbou z důvodu profesionální podpory. Má potom jistotu, že v případě technického problému není odkázána pouze na vlastní zdroje.

CentOS je přímým derivátem z produktu RHEL, nicméně je poskytován zdarma, ale také bez oficiální podpory. Jedná se o velmi populární systém. Dále lze jmenovat například Debian, Ubuntu či Fedora.

Implementace od Microsoftu staví na mnoha veřejných standardech, jako je LDAP, Kerberos či SMB (respektive CIFS), které jsou běžně využívány i v Linuxovém světě. To přímo vybízí k poskytnutí AD služeb na alternativní platformě. Již dlouho dobu se pro sdílení souborů a tiskáren využívá software Samba. Ta umožňuje veškeré potřebné funkcionality, jako jsou uživatelé, práva, logování, škálování či šifrování provozu.

6.1 CentOS 7

Při rozhodování, který systém použít, padla volba na CentOS 7. Jak již bylo zmíněno v minulé kapitole, má kvalitní základ a širokou komunitu. Nicméně není problém využít některý z dalších podporovaných a rozšířených systémů, jako je

otcovský RHEL a dále Debian, Ubuntu, Fedora či OpenSUSE (Samba project, ©2018a). Hlavním důvodem pro výběr jsou mnohaleté zkušenosti se zvolenou platformou, která se za tu dobu ukázala jako vysoce stabilní s dobrou podporou komunity, což je naprosto klíčové pro produkční nasazení. Pokud firma vyžaduje i záruky poskytnutí podpory, lze se spolehnout na RHEL.

Administrátoři systémů si v současné verzi všimnou několika zásadních změn. Jednou z nejdůležitějších je náhrada původního démona `init` za `systemd`, který spravuje systém. Oba jsou spuštěny hned na začátku a řídí celý proces startu systému, jsou rodiči všech následujících procesů a starají se o ty odloučené, tvoří `runlevely` (v `init`) / `targety` (v `systemd`), řeší závislosti a mnohé další.

Další je náhrada osvědčeného souborového systému ext4 za moderní XFS, aktualizace zavaděče systému na novější verzi či náhrada `iptables` pomocí `Firewalld`.

6.2 Samba

Možnost využívat Sambu jako doménový řadič přišla až v její verzi 4. Do té doby zde podpora nebyla a sloužila pouze jako nástroj pro sdílení souborů a tiskáren. V době psaní této práce je nejnovější hlavní verze, kterou lze stáhnout z oficiálních stránek Samby (www.samba.org), označována jako 4.8. Nicméně instalace tímto způsobem zahrnuje kompilaci balíčků administrátorem. To je mnohem méně pohodlné než využití dostupných řešení z repositářů, kde je zajištěna snadná instalace i aktualizace.

Pro zjištění dostupné verze Samby na CentOS 6/7 lze využít následující příkaz:

```
[root@centos ~]# yum list | grep samba
```

Předchozí vydání nabízelo standardně verzi 3.6.23 případně 4.2.10 (balíček `samba4`). Tudíž i zde bylo možné provozovat AD služby. V distribuci CentOS 7.5, která byla vydána v průběhu psaní této práce, Samba opět povýšila a nyní je dostupná verze 4.7.1, tedy o jednu hlavní verze pozadu než na oficiálním webu. Bohužel verze dostupná skrze repositář v sobě neobsahuje nástroj `samba-tool`, který se využívá k vytvoření nové domény.

6.2.1 Požadavky

Základním požadavkem je volba systému, kde jsou k dispozici repositáře se Sambou případně je možné ji zkompilovat.

Dále jsou potřeba vyřešit závislosti, které s ní přicházejí. Při instalaci Samby pro klasické sdílení souborů stačí zadat jeden příkaz a balíčkovací nástroj `yum` nabídne ke stažení všechny chybějící komponenty.

```
[root@centos ~]# yum install samba
```

```
Dependencies Resolved

================================================================

Package        Arch Version        Repository     Size

================================================================

Installing:

Samba          i686 3.6.23-46el6_9 updates        5.1 M

Updating for dependencies:

samba-common   i686 3.6.23-46el6_9 updates        10 M

samba-winbind  i686 3.6.23-46el6_9 updates        2.2 M

samba-winbind-clients    i686 3.6.23-46el6_9 updates   2.0 M
```

`Yum` si zjistil všechny závislosti a automaticky je nabídne ke stažení/aktualizování. Tím je celý proces hotový.

Jiná situace nastává při využití adresářových služeb. Samba pro ně potřebuje spolupráci více balíčků a je nutné se rozhodnout, jestli má server sloužit pouze jako člen domény (například využít uživatele v již existujícím systému) nebo jako řadič a tím poskytovat funkce doméně. Pro účely této práce je potřeba zvolit možnost číslo dva, tudíž před instalací samotné Samby ručně nainstalovat závislosti popsané na oficiálních stránkách (Samba project, ©2018a):

```
[root@centos ~]# yum install attr bind-utils docbook-style-
xsl gcc gdb krb5-workstation libsemanage-python libxslt perl
perl-ExtUtils-MakeMaker perl-Parse-Yapp perl-Test-Base
pkgconfig policycoreutils-python python-crypto gnutls-devel
libattr-devel keyutils-libs-devel libacl-devel libaio-devel
libblkid-devel libxml2-devel openldap-devel pam-devel popt-
devel python-devel readline-devel zlib-devel systemd-devel
```

Zde je hned několik zajímavostí. Jak bylo řečeno na začátku, pro autentizaci uživatele bude použit protokol Kerberos. Ten je zde obsažen v balíčku `krb5-workstation`. Samba dříve používala implementaci Heimdal. Software, který s touto verzí nebyl kompatibilní nemohl využít Kerberos autentizaci od Samba DC. Nově od verze 4.7 je možné použít i představenou verzi MIT Kerberos a nabídnout kompatibilitu s těmito systémy. (Samba project, ©2017a)

Další je balíček `bind-utils` představující soubor nástrojů pro práci s DNS, který je kritický pro fungování celku.

`openldap-devel` je implementace LDAPu (protokol pro přístup a manipulaci s daty, z angl. „Lightweight Directory Access Protocol“), který Samba využívá jako AD back-end.

7 Návrh implementace CentOS jako AD v heterogenních sítích

Analýza ukázala, že je možné využít CentOS 7 jako základ pro adresářové služby se zapojením softwaru Samba. Nicméně zatím není jasné, jak moc se alternativní verze bude blížit původnímu řešení od společnosti Microsoft. V současné době jsou známy některé chybějící funkcionality, jako je replikace adresáře Sysvol (Samba project, ©2017b). Ten v sobě uchovává skripty, které se spouští při přihlášení uživatele na počítači či objekty skupinové politiky, které určují, co uživatelé mohou a co mají naopak zakázané (Microsoft Corporation, ©2018a). V praxi to znamená, že Sysvol je možné konfigurovat pouze na jednom doménovém řadiči a pro zajištění vysoké dostupnosti si správce musí vyřešit replikaci jinými prostředky.

Problematický je vztah důvěry, který zde není plně podporován a chybí také kontrola SID, který zabraňuje uživatelům získat administrátorská práva při přístupu k datům z druhé domény spojené vztahem důvěry. Seznam neimplementovaných funkcí lze dohledat na oficiálních stránkách Samby. (Samba project, ©2018k)

Další nevýhodou alternativního a svobodného softwaru je to, že není „povinnost“ opravovat chyby jako by tomu mělo být u placené varianty. Tam má člověk jistotu, že případnými chybami by se autoři měli zabývat. Nicméně ani zde nezůstane administrátor odkázaný sám na sebe. Komunita okolo projektu je veliká a dokáže vyřešit mnohé problémy. Navíc samotní tvůrci Samby umožňují hlášení chyb i zasílání hotových patchů na objevené problémy. Projekt je tedy dále rozšiřován, chyby jsou opravovány kontinuálně a nic nenasvědčuje tomu, že v budoucnu by tomu mělo být jinak.

CentOS přímo vychází (ze stejného zdrojového kódu) z RHELu, tudíž i zde dochází k opravám problémů a distribuci nových funkcionalit. Oba softwary jsou vhodnými kandidáty pro produkční nasazení.

Rozhodnutí nasadit Sambu jako doménový řadič by měla předcházet důkladná analýza současného stavu IT infrastruktury a funkcionalit, které od něj budou očekávány. Využití alternativní instalace mimo jiné znamená, že software třetích stran nemusí plně fungovat s jiným doménovým řadičem. Například ještě nedávno Samba používala výhradně alternativní implementaci Kerberos.

Dalším negativem jsou vyšší nároky na IT správce. Windows Server je velmi populární a mezi administrátory mnohem známější než doména provozovaná na Linuxu.

Pokud se firma rozhodne nasadit Sambu jako doménový řadič, musí počítat s tím, že nemá všechny potřebné nástroje a mohou se v něm vyskytovat chyby. Problémy se samozřejmě můžou vyskytnout v libovolném programu, ale zde si správci budou muset některé věci vyřešit sami, viz. zmíněná replikace adresáře Sysvol.

Velké korporace se budou pravděpodobně spoléhat na řešení Windows Server a jejich oficiální podporu. To sice znamená náklady za nákup softwaru, ale na druhou stranu jsou všechny funkcionality zajištěny „out-of-the-box“ (tedy hned po instalaci).

V rámci této práce se konfigurace zaměří na menší podniky s logickým uspořádáním jednoho lesa a jedné domény, které vyhoví spoustě organizací a Samba s tímto nastavením bude mít nejméně problémů.

7.1 Topologie

Pro účely testování a provozu systému bude využit fyzický server, na kterém poběží virtuální technologie (tzv. hypervisor) VMware ESXI od společnosti VMware. Software provádí virtualizaci systémových prostředků na nejnižší úrovni a poskytuje mnohem lepší výsledky než běžná virtualizace nad operačním systémem. Díky ní je možné provozovat mnoho virtuálních počítačů, přiřazovat jim systémové prostředky (CPU, RAM, HDD, síťové připojení…), sledovat jejich stav, přistupovat k virtuální konzoli či řešit bonusové služby jako je HA. Poslední zmíněna funkcionalita bohužel není dostupná ve zdarma verzi.

Hypervisor umožňuje zapínat a vypínat jednotlivé hostované systémy nebo jim odebírat diskové jednotky, takže lze snadno nasimulovat havárii a testovat vysokou dostupnost. To vše bez toho, aby bylo potřeba více serverů případně ručně odpojovat kabely. Konfigurace je prováděna v uživatelsky přívětivé administraci.

ESXI hostitel bude obsahovat celkem tři hosty.

- Doménový řadič 1
- Doménový řadič 2

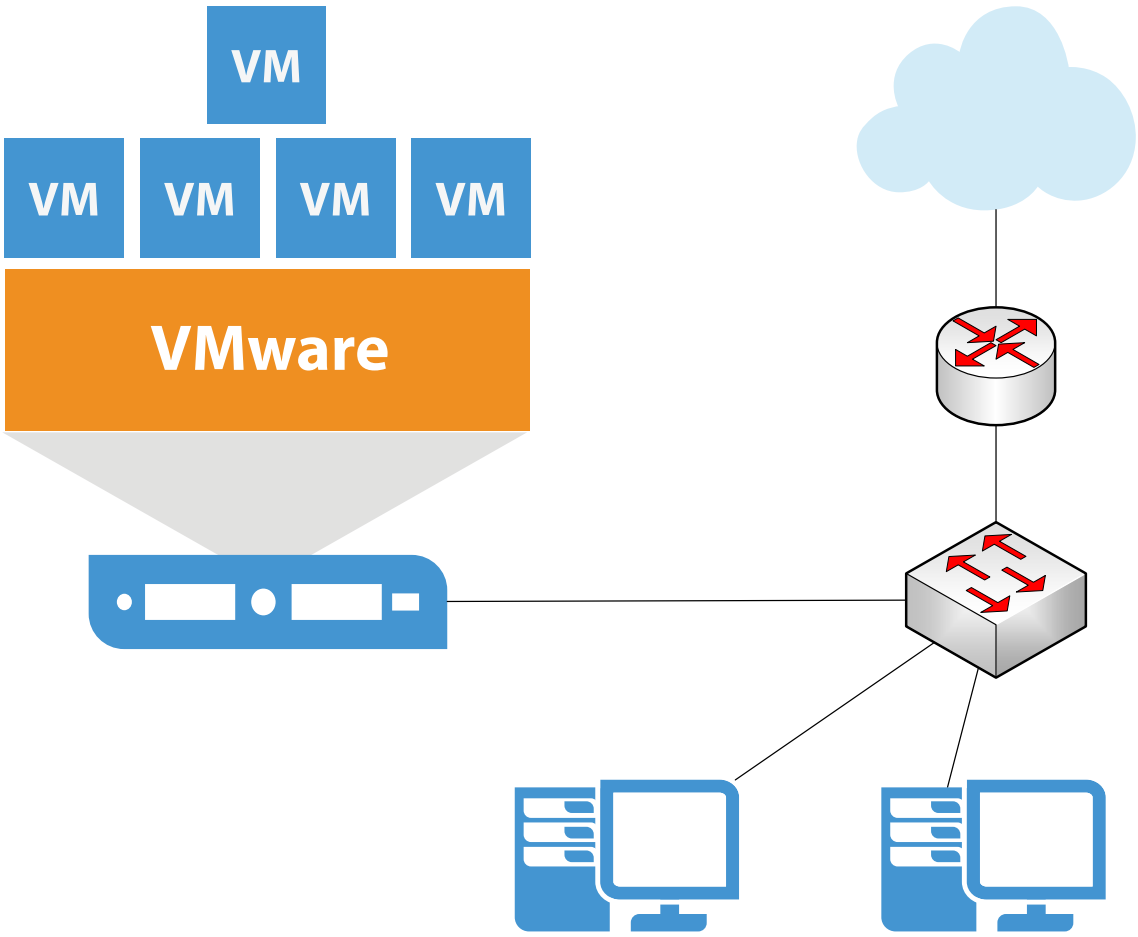
} vysoká dostupnost

- Souborový server 1
    - Zároveň poslouží jako Linuxový člen domény

Doménové řadiče spolu budou spolupracovat a výpadek jednoho neohrozí chod celé firmy, jelikož základní replikace uživatelů napříč řadiči funguje v základu. Souborový server opět obstará Samba. Ta bude připojena do domény a poskytne uživatelům možnost využít síťovou složku pro ukládání souborů. Pro vyšší bezpečnost dat a s tím související HA lze provozovat síťový disk za pomoci kernelového modulu DRBD, který poskytne „síťový raid“.

Mimo server budou k dispozici i dva počítače s operačním systémem Windows 10 Pro v 64 bitové verzi, které budou jednak sloužit jako testovací klienti pro připojení Windows stanic a jednak jako PC, kde budou umístěny administrátorské nástroje RSAT pro správu AD. V případě Windows je vhodné podotknout, že pro připojení do domény je potřeba mít minimálně verzi Pro (Windows 8, 8.1, 10) nebo Professional (Windows 7). Nicméně i u starších verzí (Vista, XP) je možné připojit počítač do domény.

Servery uvnitř ESXI mezi sebou lokálně komunikují, nicméně pro připojení do sítě bude potřeba i switch, který propojí server a počítače, případně další fyzické zařízení, které by se do testovacího prostředí přidalo.



Obrázek 5 - Schéma testovacího prostředí pro adresářové služby

Výhoda využití virtualizace je z obrázku (Obrázek 5) patrná. Jeden fyzický server pojme většinu testovacího prostředí. Mohlo by i celé, ale pak by bylo potřeba zakoupit licenci Windows 10 Pro a nainstalovat ji jako šestý virtuální stroj.

V reálném nasazení by pro dosažení vysoké dostupnosti musely být tyto virtuální systémy rozmístěny na různých serverech. Produkční sestava by se mohla skládat ze dvou fyzických serverů s hypervisorem a na každém z nich by běžel jeden doménový řadič a jedno sdílení souborů oba propojené do HA.

8 Stanovení výchozích hypotéz

Tato práce si bere za úkol prozkoumání možností využití alternativního řešení služeb Active Directory na platformě Linux. Jelikož uživatelé nepoužívají pouze platformu Windows, bude systém nasazen v heterogenním prostředí, a to včetně vysoké dostupnosti.

8.1 Hypotéza 1

Funkce poskytované doménovým řadičem budou provozovány v režimu vysoké dostupnosti. Porucha jednoho tedy neohrozí fungování zbytku sítě.

8.2 Hypotéza 2

Doménový řadič umožní připojení a přihlášení klientského PC s Windows 10 Pro 64 bit a CentOS 7 64 bit do domény.

8.3 Hypotéza 3

Počítače s OS Windows budou využívat doménové politiky nastavené správcem, jako je například automatické připojení síťového disku.

9 Realizace řešení

Předpokladem pro nasazení systému je již fungující síť s připojením do internetu. U serverů nezáleží, zda je nebo není použito virtualizované prostředí. To záleží na konkrétním nasazení, požadavcích zákazníka a správce.

Druhou podmínkou je využití CentOS 7 64 bit v serverové části i jako klienta a dále dva počítače s Windows 10 Pro 64 bit pro testovací účely. Jeden z nich bude zároveň hostitelem RSAT, kterými bude AD spravováno.

Pro nasazení doménových služeb na CentOS jsou předpokládány minimálně základní zkušenosti správce s nasazením, konfigurací a provozem Linuxového operačního systému. Dále znalost síťové problematiky pro propojení zařízení a zkušenosti se samotným Windows 10, aby jej bylo možné připojit do domény.

Výběr použitého serverového softwaru a jeho verze:

- CentOS 7.5.1804 x86_64
- Samba 4.7.7
- Krb5-workstation 1.15.1-19
- NTP 4.2.6p5-28

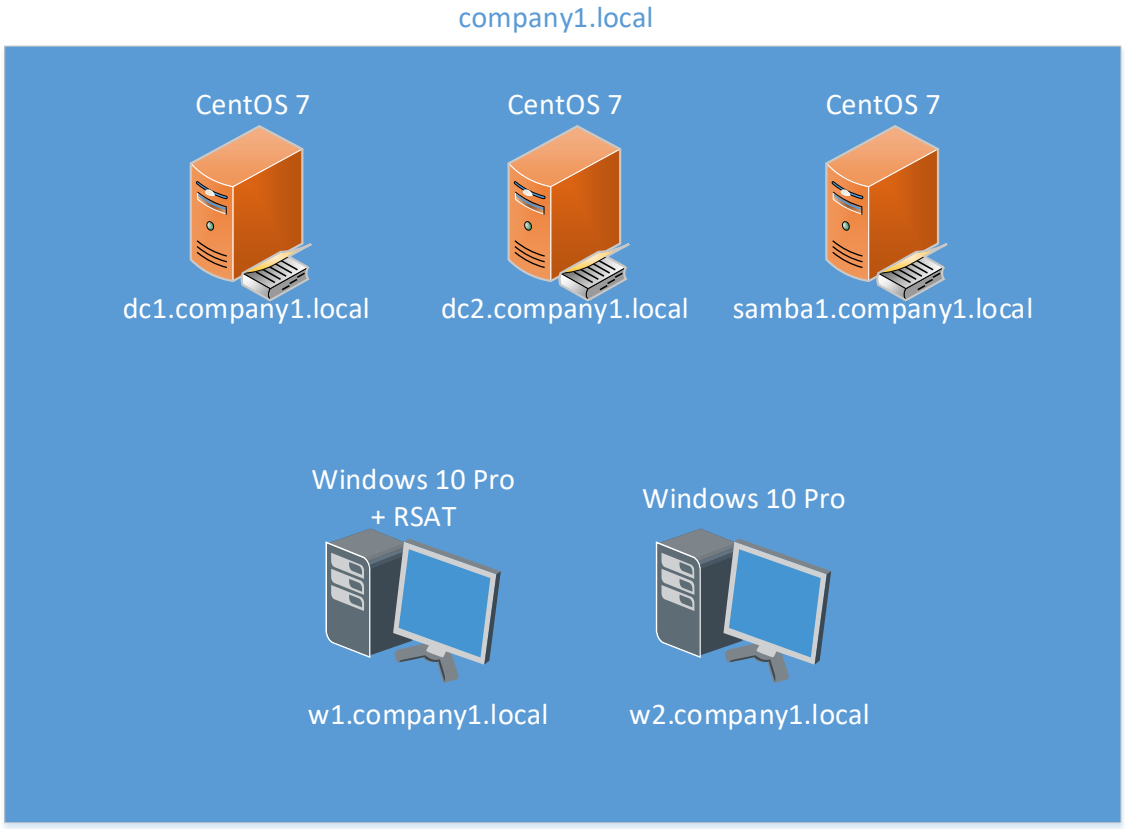
Je potřeba zdůraznit, že v rámci zabezpečení bude použit firewall, ale zároveň bude deaktivován SELinux na všech serverech, který podrobně řeší použitá práva.

Na všech Linuxech je přístupný účet root a veškerá konfigurace bude prováděna právě pomocí tohoto účtu.

9.1 Schéma rozdělení

Jak již bylo řečeno, Active Directory silně spolupracuje s DNS a využití systému zahrnuje definici doménových názvů. Každé zařízení, ať je to router, server nebo počítač, zapojené do domény má unikátní název, tzv. FQDN (plně kvalifikovaný doménový název, z angl. „Fully Qualified Domain Name“). Například počítač 1 může být v doméně označen jako pc1.firma.cz. Skládá se tedy z názvu zařízení a doménové přípony. (Stanek, 2009 stránky 24-26)

Pro testovací prostředí bude využita doména company1.local s doménovými řadiči dc1 a dc2. Schéma je znázorněno na následujícím obrázku (Obrázek 6, str. 32).



Obrázek 6 - Doménové schéma v company1.local

9.2 Úvodní konfigurace dc1.company1.local

Následující podkapitoly čerpají především z oficiálních stránek výrobce softwaru Samba. (Samba project, ©2018c), (Samba project, ©2018a)

9.2.1 NTP

První server zapojený do domény a zároveň její řadič bude označen jako dc1.company1.local. Po základní instalaci CentOS je nutné provést několik kroků, než se nasadí Samba.

Úplně na začátku je třeba zajistit synchronizaci času. Na jeho přesnosti závisí funkčnost celé domény. Jeden z prvků, pro který je kriticky důležité mít aktuální informaci je Kerberos. Ten neustále pracuje s časem a pokud ho zařízení nemají správně nastavený, nedojde k autorizaci a autentizaci požadavků. Tím se naruší provozuschopnost celého systému. (Ricciardi, 2007)

Nejedná se jen o Kerberos jako takový, ale časové rozdíly působí problémy i při replikaci mezi DC. Řadiče neví, který záznam je aktuální a synchronizace selže. (Samba project, ©2018b)

Pro zajištění přesného času se použije NTP (internetový časový protokol, z angl. „Network Time Protocol“). Ten slouží k synchronizaci se servery poskytujícími aktuální data. Instalace se provede příkazem:

```
[root@dc1 ~]# yum install ntp
```

Po instalaci lze v souboru `/etc/ntp.conf` editovat poskytovatele. V základu je zde odkaz na `centos.pool.ntp.org`, ze kterých je následně přiděleno konkrétní internetové zařízení. Nastavení lze nechat v základu nebo je možné využít české servery, jako jsou `ntp.nic.cz`, `tik.cesnet.cz` nebo `tak.cesnet.cz`. Přidaný parametr `iburst`, který se nachází v konfiguračním souboru, se postará o rychlejší počáteční synchronizaci.

Mezi přidané parametry patří i název adresáře, pro podepsané NTP sockety. Windows stanice nepřijmou běžný požadavek na úpravu času, ale pouze podepsaný od doménového řadiče.

```
ntpsigndsocket /usr/local/samba/var/lib/ntp_signd/
```

Na závěr se aktivuje automatický start služby pomocí příkazu:

```
[root@dc1 ~]# systemctl enable ntpd
```

Nicméně start `ntpd` neproběhl tak, jak byl zamýšlen. Zjistilo se, že při startu systému se v CentOS 7 spustí služba `chronyd`. Jedná se nástroj, který také poskytuje časovou synchronizaci, ale pro účely AD se zvolil program `ntpd`. Proto při startu serveru dojde ke spuštění `chronyd`, který zablokuje udp port 123 a tím se nespustí `ntpd`. Deaktivace se provede následovně.

```
[root@dc1 ~]# systemctl disable chronyd
```

9.2.2 EPEL

Za účely testování bude využita novější verze programu Samba. Ta je v rámci standardního repositáře pro CentOS dostupná jako 4.7.1, přičemž na oficiálních stránkách byla v době psaní této práce 4.8.2. Je tedy nutné získat a zkompilovat zdrojové kódy pro konkrétní platformu.

Při instalaci z repositáře dojde k automatickému stažení všech potřebných závislostí. Jedná se o velkou výhodu, jelikož systém za něj vyřeší vše potřebné a systém se následně snadno udržuje v aktuálním stavu. To v případě ruční kompilace není možné a správce si vše musí zařídit sám. Naštěstí autoři softwaru myslí i na toto a nabízí seznam potřebných závislosti pro jednotlivé Linuxy. Více informací lze nalézt v kapitole 6.2.1 Požadavky

Mimo ně je vhodné nainstalovat ještě `cups`, pro případný management tiskáren a `BIND` pro pokročilé DNS. Více v kapitole 6.2.1 Požadavky.

Bohužel i kdyby někdo chtěl využít verzi dostupnou z oficiálního repositáře, tak nebude mít k dispozici nástroj `samba-tool`, který je klíčový pro nastavení a ovládání Samby v režimu AD.

Některý software nelze získat ze standardního repositáře. Známé alternativní uložiště se nazývá EPEL a v nové verzi CentOS ho lze nainstalovat velice jednoduše.

```
[root@dc1 ~]# yum install epel-release
```

Nyní jsou k dispozici veškeré potřebné programy.

9.2.3 Změna názvu

S využitím doménových služeb je potřeba změnit označení serveru na FQDN. K tomu se upraví název v souboru `/etc/hostname`.

```
dc1.company1.local
```

Dále se přidá řádek do `/etc/hosts`, kde IP adresa odpovídá tomuto zařízení.

```
192.168.130.10  dc1.company1.local
```

Pro zohlednění změn doménového jména je potřeba server restartovat příkazem `init 6`.

9.2.4 Samba

Ke stažení slouží nástroj `wget`. Pokud není k dispozici, lze ho přes `yum` doinstalovat stejně jako `ntp`. Stažení a rozbalení souboru:

```
[root@dc1 inst]# wget
https://download.samba.org/pub/samba/stable/samba-
4.7.7.tar.gz

…

[root@dc1 inst]# tar -xvf samba-4.7.7.tar.gz
```

Následně se pomocí `cd` přejde do nově vytvořené složky `samba-4.7.7` a zadá se příkaz.

```
[root@dc1 samba-4.7.7]# ./configure
```

`configure` je nutný krok k samotné kompilaci. Má za úkol nastavit potřebné cesty, aktivovat/deaktivovat volitelné funkcionality a součásti. Vytvoří soubor s konfigurací, který je dále předán.

Například je možné zakázat sdílení tiskáren přes službu `cups` nebo zvolit MIT implementaci Kerbera místo Heimdal.

Po provedení se spustí samotná kompilace `make`, která využije výstup z `configure`. Tento krok je časově náročnější, ale naštěstí jej lze pomocí parametru „j“ paralelizovat v prostředí s víceprocesorovými jádry.

Poslední krokem je samotná instalace. Té může předcházet `make test`, který ověří výsledek programu `make`, ale není nutné ho provádět. Zde jsou veškeré zkompilované soubory přesunuty na své finální místo a program je připraven k provozu.

```
[root@dc1 samba-4.7.7]# make install
```

Jelikož software nebyl instalován ze standardního repositáře CentOS, ale ruční kompilací, tak nemá stejné rozmístění souborů. Systému se musí říct, kde má hledat ovládací skripty a na to slouží proměnná `PATH` (vypsání pomocí `$PATH`). Stačí editovat soubor `~/.bashrc`, na konec přidat cestu k novým programům a restartovat server.

```
export
PATH=$PATH:/usr/local/samba/bin/:/usr/local/samba/sbin/
```

Na závěr je nutné smazat konfigurační soubor Kerbera v `/etc/krb5.conf`. Pokud se tento krok neprovede, obdrží uživatel v dalším postupu chybovou hlášku. Následně se využije nový `krb5.conf`, který Samba vygeneruje v průběhu založení doménového řadiče.

Nyní jsou hotovy všechny předpoklady pro fungování a zbývá nakonfigurovat samotnou Sambu pro její novou roli. V průběhu delegace doménového řadiče bude program interagovat se správcem pro zadání vstupních dat. Naštěstí je instalace velice chytrá a nabídne výchozí hodnoty, kterou považuje za správnou v daném systému.

Samotný proces je modifikován parametrem `--use-rfc2307`. Ten popisuje možnost využití LDAP jako adresáře pro uchování informací o uživatelích a skupinách. V praxi to znamená nastavení domovských adresářů, přiřazení uživatelů do skupin nebo typ shellu. (Samba project, ©2018e) a (Howard, 1998)

```
[root@dc1 ~]# samba-tool domain provision --use-rfc2307 --
interactive
```

Parametr `--interactive` způsobí postupné dotazování uživatele na hodnoty.

```
Realm [COMPANY1.LOCAL]:
```

Hodnota v hranatých závorkách je výchozí, která bude použita, pokud nedojde k zadání jiného údaje. Pokud nebude uvedeno jinak, bude využita právě tato defaultní.

Pojem `realm` označuje tzv. `Kerberos realm`. Jedná se o oblast, kde zařízení využívají společnou Kerberos databázi a dokáží využívat vztahu důvěry. (Stanek, 2009 str. 254) Zde je aplikován princip tiketů popisovaný v kapitole 4.4.1 Kerberos.

```
Domain [COMPANY1]:
```

Z názvu je patrné, že zde bude uvedena doména, do které tato instalace spadá.

```
Server Role (dc, member, standalone) [dc]:
```

Nyní se určí, jako roli bude server vykonávat. Jelikož nejdříve je potřeba doménový řadič, nechá se výchozí hodnota `dc`. `Member` označuje zařízení připojení do domény, které ale nevykonává funkci řadiče. `Standalone` není do domény ani zapojen.

Pomocí `samba-tool` má být prováděno pouze vytvoření nového/připojení dalšího doménového řadiče (obecně práce s DC). Ostatní možnosti budou v dalších verzích odstraněny a nástroj bude sloužit jen k výše zmíněnému účelu. Pro připojení serveru pouze jako člena domény se použije příkaz `net ads join`. (Samba project, ©2018k), (Samba project, ©2018l)

```
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]: BIND9_DLZ
```

Následuje volba DNS mechanizmu, který bude fungovat na pozadí celého systému. Pro novou instalaci v jednoduchém prostředí bez znalosti služby BIND (DNS server) je doporučeno použít interní Samba DNS, který nepotřebuje dodatečné nastavení. Nicméně má i své limity, které by si každý správce měl nastudovat a rozhodnout se, co je pro konkrétní nasazení nejlepší. Je možné začít s interním DNS v Sambě a následně přejít na robustnější řešení BIND. Transformaci je možné provést i při nasazeném AD. Pokud jsou plánované pokročilejší DNS služby nebo komplexnější AD schéma, je vhodné rovnou použít BIND. (Samba project, ©2018f)

`DNS forwarder` je adresa serveru, kam budou přeposlány veškeré požadavky, které nedokáže interní DNS systém Samby vyřešit. Může zde být jiný DNS server v síti nebo veřejné dostupné, například Google. Uživatel ho zadává pouze v případě `SAMBA_INTERNAL`. Pro `BIND9_DLZ` tato volba není k dispozici a nastavuje se ručně v `named.conf`.

Posledním krokem je zadání hesla doménového administrátora. To podléhá určitým kritériím na počet znaků a jejich výskyt. Na základě vstupních dat Samba provede potřebnou konfiguraci.

Nyní se zkopíruje nově vytvořený `krb5.conf` na místo dříve smazaného a nastaví se mu potřebná práva.

```
[root@dc1 ~]# cp /usr/local/samba/private/krb5.conf /etc/
[root@dc1 ~]# chown root:named /etc/krb5.conf
```

Bohužel na testovacím serveru nedošlo k vytvoření složky `/usr/local/samba/var/lib/ntp_signd/`, kterou využívá `ntpd`. Je tedy nutné ověřit, zda existuje pomocí příkazu `ls /usr/local/samba/var/lib/`. Pokud ne, tak ji ručně vytvořit a ověřit, že má příslušná práva (výstup zkrácen).

```
[root@dc1 ~]# mkdir /usr/local/samba/var/lib/ntp_signd

[root@dc1 ~]# chown root:ntp
/usr/local/samba/var/lib/ntp_signd/

[root@dc1 ~]# chmod 750 /usr/local/samba/var/lib/ntp_signd/

[root@dc1 ~]# ls -la /usr/local/samba/var/lib/

drwxr-x--- 2 root ntp  20 Jun  5 22:23 ntp_signd
```

9.2.5 DNS a firewall

Jelikož byl zvolen BIND jako DNS server, bude potřeba ručně upravit konfigurační soubory. V případě použití `SAMBA_INTERNAL` volby při zavedení domény odpadá starost s další konfigurací.

Systém DNS je potřeba upravit souborem `/etc/resolv.conf`, který obsahuje záznamy pro překlad adres. Nejprve je ale nutné zakázat `NetworkManager`, aby tento soubor nadále nepřepisoval, a to zadáním parametru `dns=none` do sekce `main` v souboru `/etc/NetworkManager/NetworkManager.conf`

Následně se do `resolv.conf` zapíše:

```
search company1.local

nameserver 192.168.130.10
```

Kde IP adresa u `nameserver` označuje tento server. `Resolv.conf` udává seznam DNS serverů, kde má systém vyřizovat své dotazy.

Poté přichází na řadu konfigurace služby BIND, která je mírně komplikovanější. Balíčky jsou nainstalovány z kapitoly 6.2.1 Požadavky a 9.2.2 EPEL. Soubor s nastavením se nachází v `/etc/named.conf` a jsou zde obsaženy informace o adresách, které se můžou dotazovat tohoto serveru, kam má přeposílat dotazy, pokud je neumí vyřešit, nastavení zón a odkazy na další soubory, které se mají zapojit.

Zóna může být celá doména, ale i jen její část a v rámci ní se nachází autoritativní server, který je hlavním pro danou zónu. Další DNS servery ho mohou využívat nebo být jeho replikou pro vysokou dostupnost. (Stanek, 2009 stránky 25-26)

Konfiguraci lze využít z oficiálních stránek projektu Samba. Je zde popsáno jak nastavení služby BIND, tak i vytvoření souborů se zónami a úpravou práv na příslušných částech systému. (Samba project, ©2018g)

Následně dojde na nastavení modulu BIND9_DLZ, který byl použit při vytvoření domény na dc1.company1.local. Samba, Kerberos a BIND dokáží automaticky udržovat zóny v rámci AD aktuální. Slouží k tomu nastavení pro zmíněný modul popsané opět na projektu Samba. (Samba project, ©2018h)

Tato Linuxová distribuce využívá `firewalld` jako software pro služby firewallu a pro správnou funkci AD je potřeba povolit porty uvedené v tabulce (Tabulka 1, str. 40).

Aplikace pravidla se provede následujícím příkazem s příslušným portem, tcp/udp spojením.

```
[root@dc1 ~]# firewall-cmd --permanent --zone=public --add-
port=53/tcp

[root@dc1 ~]# firewall-cmd --reload
```

Tabulka 1 - seznam portů pro provoz služeb AD. Převzato a upraveno z (Samba project, ©2018d)

Služba	Port	Protokol
DNS	53	tcp/udp
Kerberos	88	tcp/udp
ntp	123	udp
End Point Mapper (DCE/RPC Locator Service)	135	tcp
NetBIOS Name Service	137	udp
NetBIOS Datagram	138	udp
NetBIOS Session	139	tcp
LDAP	389	tcp/udp
SMB over TCP	445	tcp
Kerberos kpasswd	464	tcp/udp
LDAPS	636	tcp
Global Catalog	3268	tcp
Global Catalog SSL	3269	tcp
Dynamic RPC Ports	49152-65535	tcp

Posledním krokem je aktivace služby při startu systému.

```
[root@dc1 ~]# systemctl enable named

[root@dc1 ~]# systemctl start named
```

9.2.6 Systemd soubory

V této fázi je server připravený vykonávat roli doménového řadiče. Poslední nastavení se týká samotného spouštění. CentOS 7 používá `Systemd` místo dřívějšího `init` jako rodiče všech procesů. Spuštění Samby bude provedeno na základě ovládacího souboru, tzv. `unit file`. (Red Hat, Inc., ©2017 stránky 119-120)

Tyto soubory se nachází ve složce `/etc/systemd/system/`. Do ní se vytvoří nový soubor, např.: `samba_ad.service` s požadovaným nastavením. Systém si při startu prostředí (`target`) načte tyto soubory a vyhodnotí pořadí spouštěných programů s celou konfigurací. Nová služba může vypadat následovně:

```
[Unit]

Description=Samba Active Directory Domain Controller

After=network.target remote-fs.target nss-lookup.target

[Service]

Type=forking

ExecStart=/usr/local/samba/sbin/samba -D

PIDFile=/usr/local/samba/var/run/samba.pid

ExecReload=/bin/kill -HUP $MAINPID

[Install]

WantedBy=multi-user.target
```

Konfigurační soubor převzat z oficiálního manuálu. (Samba project, ©2017d)

Zde je vhodné provést změnu oproti oficiálnímu doporučení. Jelikož ke službě AD neodmyslitelně patří synchronizace času a DNS, je vhodné doplnit do parametru `After` tyto hodnot: `named.service ntpd.service`

Tím se systému řekne, aby nejprve spustil `named` (BIND DNS) a `ntpd` (synchronizace času) a poté spustil Sambu.

Na závěr se může spustit doménový řadič dc1.company1.local.

```
[root@dc1 ~]# systemctl enable samba_ad

[root@dc1 ~]# systemctl start samba_ad
```

9.2.7 Samba 4.8.2

Samba 4.7.7 netvoří poslední vydání. V době psaní této práce to byla verze 4.8.2. Bohužel toto vydání přineslo komplikace s nasazením AD. Při vytváření domény proces proběhl s výstražnou hláškou.

```
Unable to determine the DomainSID, can not enforce uniqueness
constraint on local domainSIDs
```

Samba vytvořila doménové prostředí, ale při pokusu o připojení druhého doménového řadiče nastala stejné chyba.

Zmíněný problém se nepodařilo vyřešit žádným způsobem. Chybu lze dohledat při použití vyhledávače Google, ale jednoznačné řešení se nepodařilo najít.

Z tohoto důvodu byla zvolena poslední aktualizace z minulé majoritní verze 4.7, konkrétně 4.7.7 datovaná k 17. dubnu 2018. (Samba project, ©2018j)

9.3 Úvodní konfigurace dc2.company1.local

Provoz pouze jednoho doménového řadiče je velké potencionální riziko pro každou společnost. V případě jeho poruchy dojde k ochromení celého systému. Je tedy silně doporučené provozovat více takových, fyzicky jiných, serverů.

Ovšem nemusí se jednat pouze o zálohu. Systém může být navržen tak, že každý server má na starosti jinou část AD nebo je rozložené působení FSMO rolí. To v případě malých podniků nemá valný význam. Tam jde především o replikaci z důvodu případné poruchy.

Druhým zařízením, které se bude podílet na provozu je dc2.company1.local. Postup konfigurace oproti dc1 bude mírně odlišný. První server zakládal nové schéma pro les a doménu. Každý další server ve stejné doméně se musí připojit do existujícího systému.

Nejprve je potřeba nainstalovat software Samba. Využije se k tomu postup z kapitoly 9.2 Úvodní konfigurace dc1.company1.local. Rozdíly oproti konfiguraci `dc1` jsou následující.

9.2.5 DNS a firewall (za využití modulu `BIND9_DLZ`).

Před konfigurací Samby se provede částečná konfigurace DNS. Nastaví se `nameserver` v souboru `resolv.conf`, aby bylo možné kontaktovat originální řadič domény.

```
search company1.local

nameserver 192.168.130.10     #dc1.company1.local

nameserver 192.168.130.11     #dc2.company1.local
```

Tímto způsobem bude možné najít službu Kerberos při pokusu o připojení, která je nyní na `dc1`. (Samba project, ©2018i)

Dále se může nastavit firewall pro bezproblémové spojení.

Poté se provede napojení Samby do již fungující domény pomocí postupu popsaného níže a dokončí se konfigurace DNS.

9.3.1 Samba

Po úspěšném přednastavení služby BIND a modulu BIND9_DLZ přichází na řadu připojení druhého doménové řadiče. Předpokladem je správně nastavený název serveru, soubor `resolv.conf`, `ntpd` a firewall.

Pokus o kontaktování domény company1.local.

```
[root@dc2 ~]# samba-tool domain join company1.local DC -
U"COMPANY1\administrator" --dns-backend=BIND9_DLZ --
option='idmap_ldb:use rfc2307 = yes'
```

Po úspěšném nalezené řadiče dc1 je uživatel vyzván k zadání administrátorského hesla dané domény. Následně Samba provede spojení, úvodní konfiguraci a replikuje základní data. Výsledkem je soubor `/usr/local/samba/private/krb5.conf`, který je potřeba opět zkopírovat do `/etc/` se skupinovými právy pro uživatele `named`. Dále soubor `named.conf` a `dns.keytab` v `/usr/local/samba/private`. Zde je opět nutné prověřit práva dle návodu pro BIND (Samba project, ©2018g). Poslední záznam z konfigurace má vypadat následovně (s odlišným SID).

```
Joined domain COMPANY1 (SID S-1-5-21-2592708054-1867127209-
952555461) as a DC
```

Nyní doména obsahuje dva řadiče. Na závěr se dokončí nastavení služby BIND, proměnné `PATH` a společně s `ntpd` a `samba_ad` je spustit.

9.4 Replikace

V současném stavu fungují servery dc1 a dc2 jako řadiče pro doménu company1.local. Nicméně jak bylo zmíněno v kapitole 7 Návrh implementace CentOS jako AD v heterogenních sítích, tak ani v nejnovější verzi není dostupná replikace adresáře Sysvol.

V základu Samba synchronizuje obsah AD mezi řadiči. To znamená vysokou dostupnost uživatelských účtů nebo DNS záznamů. Pro zbylé záležitosti je potřeba replikaci vyřešit jiným způsobem. Například pomocí nástroje `rsync`. (Samba project, ©2018k)

Program `rsync` slouží především ke vzdálenému kopírování souborů mezi servery. S oblibou je využíván jako zálohovací nástroj, který umí uchovávat atributy u souborů a dokáže přenášet pouze změny. Díky tomu je zpravidla druhé a další kopírování pomocí `rsync` rychlejší než to první, kdy se musí přenést vše.

V praktickém použití to znamená, že určité úpravy (například konfigurace skriptů po přihlášení) bude možné dělat pouze na jednom, předem vybraném, DC. Ten se následně postará o distribuci změn na další servery. Nemělo by se jednat o velkou překážku, nicméně je na to potřeba myslet, jelikož změny udělané na jiném DC nebudou replikovány a při nejbližší synchronizaci dojde k jejich přepsání.

Na všech server v doméně je potřeba nainstalovat `rsync` pomocí `yum`. Dále se vybere jeden hlavní, na kterém se bude provádět konfigurace. Zde to bude dc1.company1.local. Pro usnadnění celkové správy byl na serverech zřízen přístup do dc2 za pomocí privátního/veřejného klíče a nemusí tedy používat hesla. Konkrétní implementace záleží na správci.

Poté je potřeba vytvořit spouštěcí skript `/usr/local/backup_scripts/startSyncSysvol` s následujícím obsahem.

```
#!/bin/bash

#Zahájí synchronizaci sysvol na zadaný server

/usr/local/backup_scripts/syncSysvol 192.168.130.11
```

V něm budou definované jednotlivé doménové řadiče, kam má probíhat replikace `Sysvol`.

Druhý soubor definuje samotné kopírování, jež musí proběhnout s udržením ACL a rozšířenými atributy souborů (parametry `-X` a `-A` u `rsync`).

```
#!/bin/bash

#Provede synchronizaci sysvol na server v parametru $1

SYSVOL=/usr/local/samba/var/locks/sysvol/

/usr/bin/rsync -aAX --delete $SYSVOL root@$1:$SYSVOL
```

Následuje změna práv.

```
[root@dc1 backup_scripts]# chmod 777 startSyncSysvol

[root@dc1 backup_scripts]# chmod 777 syncSysvol
```

Poslední krok je automatizace procesu s `crontab`. V něm lze definovat úlohy, které mají pravidelně probíhat. Tedy kupříkladu replikace `sysvol` každých pět minut. Editace se provede pomocí `crontab -e` a obsah bude vypadat takto.

```
5 * * * * /usr/local/backup_scripts/startSyncSysvol
```

Nyní jsou doménové řadiče připraveny k poskytování AD služeb na platformě Samba ve vysoké dostupnosti.

9.5 Připojení Windows stanice

V této chvíli je možné využít instalované řadiče pro doménové přihlášení. Uživatelé mohou pomocí svých údajů přejít z jednoho počítače na jiný a přihlásit se pod stejným uživatelským jménem a heslem. Zároveň správce může řídit skupinovou

politiku a centrálně řídit veškeré potřebné nastavení, které bude následně distribuováno skrze vytvořenou doménu.

9.5.1 Požadavky

V kapitole 7.1 Topologie bylo řečeno, že nelze využít verze Windows určené pro domácí použití, ale musí být k dispozici vyšší řady. Konkrétně u testovacích počítačů se jedná o Windows 10 Pro 64 bit build 10.0.17134.

Předpokládá se viditelnost doménového řadiče pro připojovaný počítač. To znamená nastavit DNS záznamy odpovídající na dc1 (hlavní) a dc2 (alternativní). V případě fungující sítě, kde je již DNS server v provozu, stačí zadat pravidlo na předávání dotazů (`*.company1.local`) na dc1/dc2. Poté se nemusí měnit nastavení na počítačích a ty využijí stávající DNS zařízení, které požadavky předá. Zde je seznam záznamů potřebných k provozu (Rahman, 2014).

Samotné připojení se provede kliknutím pravého tlačítko myši na `Tento počítač`, `Vlastnosti` a následně volba `Změnit nastavení` v sekci `Nastavení názvu počítače, domény a pracovní skupiny`. Zde je zobrazen současný stav, který lze editovat tlačítkem `Změnit`. Následně stačí zaškrtnout volbu `Domény:` a zadat `company1.local`. Po potvrzení se vyšle DNS dotaz na zjištění informací o doméně včetně zjištění dostupných doménových řadičů a uživatel je vyzván k zadání údajů administrátora. Ten má standardně právo připojovat nové počítače do domény. Jeho přihlašovací jméno bude, stejně jako údaj jiných uživatelů, vypadat následovně.

```
Uživatelské jméno: administrator@company1.local
```

Po úspěšném spojení je nutné restartovat počítač k aplikování změn. Následně by se pod přihlašovacím oknem měla zobrazit informace, k jaké doméně se zadané uživatelské údaje vztahují. Jinou (například přihlášení do lokálního účtu) lze zadat ve tvaru `doména\uživatel` nebo `uživatel@doména`.

9.5.2 Remote Server Administration Tools

Microsoft nabízí možnost spravovat Active Directory přímo z Windows klientů bez nutnosti připojit se na virtuální plochu serverového prostředí. Nástroj k tomu

určený se nazývá RSAT a lze jej nainstalovat na zmíněné Windows 10 Pro. Po přihlášení na účet administrátora a instalaci softwaru získá možnost spravovat uživatelské účty a skupiny, sdílení souborů včetně nastavení práv, skupinovou politiku a obecně přehled na vytvořenou doménou. (Microsoft Corporation, ©2017a)

Prvním krokem by měla být definice uživatele, který bude přistupovat k systému a vyzkoušet na něm příslušné funkcionality. Správu poskytne aplikace `Uživatelé a počítače služby Active Directory` (`UMAC`) skrze nabídku `Start`. Bohužel od verze Windows 10 Microsoft ztížil ovládání AD na platformě Linux. RSAT zde nepodporují možnost `Server for NIS Tools` pomocí které se nastavovaly UNIXové atributy uživatelům (Microsoft Corporation, ©2018e). Jedná se o zásadní problém, který komplikuje práci správcům systému. Znamená to, že je potřeba si externě hlídat číselnou řadu pro `uid` a `gid`, kterou si dříve spravovalo přímo AD. Tyto identifikátory se používají k jednoznačné identifikaci uživatelů (`uid`) a skupin (`gid`) v rámci Linuxového systému. Pro editaci se povolí v horním menu `Zobrazit` volba `Upřesňující funkce`. Ta zpřístupní editaci všech atributů u objektů v AD a správce má opět možnost definovat správné hodnoty dle specifikace rfc2307 (Samba project, ©2018e), (Samba project, ©2018m), (Howard, 1998). Hodnoty `uid` (`uidNumber` atribut v AD) a `gid` (`gidNumber` atribut v AD) musí odpovídat rozsahu definovaném na souborovém serveru popsaném v kapitole 9.6 Souborový server. V opačném případě nedojde ke správnému mapování hodnot a Linux nebude moci využít uživatelů v doméně. (Red Hat, Inc., ©2017 stránky 256-257)

Druhým užitečným nástrojem je `Správa zásad skupiny`. Zde se definují jednotlivá pravidla. Například, že se všem uživatelům po přihlášení automaticky připojí síťový disk „`R`“ odkazující na sdílení poskytnuté Sambou ze souborového serveru. Přístupová práva lze vyřešit pomocí `Správa počítače`, kde je v menu položka `Akce` a `Připojit k jinému počítači` – Sambě. Aby nemuseli nic zadávat, použije se cachované přihlašovací údaje. Jednoduché, ale velice praktické řešení.

Všechny tyto možnosti představují efektivní správu celého systému. Ten je navíc distribuovaný na více serverech, takže omezuje riziko ztráty dat a nabízí možnost využívat jeho údaje pro další účely, a to ve formě napojení aplikací třetích stran, které

si získávají uživatele z AD. Takovým produktem může být emailový server, který přebírá definici objektů ze zmíněného systému a tím zabraňuje duplikaci a rozdílnosti dat v různých aplikacích.

9.6 Souborový server

Výhod prostředí Active Directory je mnoho oproti lokálnímu nastavení na každém počítači. Administrátor může centrálně spravovat velkou část firemní IT infrastruktury, přičemž reálný užitek mají i samotní uživatelé. Mohou využít doménového přihlášení, které je k dispozici po konfiguraci řadiče dc1 a dc2 popsané v minulých kapitolách.

Dalším základním benefitem může být automatická konfigurace sdílené složky, kterou mají pracovníci společně k dispozici pro ukládání firemních dat. Pokročilejší funkce, kterou mohou využívat je síťový domovský adresář a roamingový profil.

Domovský adresář nabízí možnost uchování libovolných souborů, který uživatel do příslušné složky umístí, přímo na serveru poskytující službu sdílení souborů. Ty mohou být (a měly by být) centrálně zálohovány a tím chráněny při případné poruše nebo ztrátě zařízení. Navíc při přihlášení na jiném počítači jsou mu všechna jeho data opět k dispozici.

Roamingový profil umožňuje automaticky ukládat konfiguraci uživatelského účtu na server. Jeho nastavení je staženo při přihlášení do počítače a nahráno zpátky při odhlášení (známé jako synchronizace cestovního profilu uživatele).

9.6.1 Konfigurace

V prvním kroku je potřeba opět upravit některé systémové soubory. Nejprve `/etc/hostname` na hodnotu `samba1.company1.local`.

Následně `/etc/hosts` s přidáním záznamu `192.168.130.12 samba1.company1.local samba1`

Větší úprava je nastavení DNS serverů, které budou řešit dotazy na překlad a to v `/etc/resolv.conf`. Předtím je nutné deaktivovat `NetworkManager`, který zmíněný soubor sám přepíše parametrem `dns=none` v sekci `main` v souboru `/etc/NetworkManager/NetworkManager.conf` a restartovat ho.

```
[root@samba1 ~]# Systemctl restart NetworkManager
```

Poté lze upravit soubor `resolv.conf`.

```
search company1.local

nameserver 192.168.130.10

nameserver 192.168.130.11
```

Dále je nutné upravit pravidla pro firewall dle následující tabulky.

Tabulka 2 - seznam portů pro provoz člena domény. Převzato a upraveno z (Samba project, ©2017g)

Služba	Port	Protokol
End Point Mapper (DCE/RPC Locator Service)	135	tcp
NetBIOS Name Service	137	udp
NetBIOS Datagram	138	udp
NetBIOS Session	139	tcp
SMB over TCP	445	tcp

Poslední krok před instalací zahrnuje aktivaci NTP pro bezproblémové fungování služeb závislých na čase (případně stáhnutí přes `yum`). Konfigurace klienta je jednodušší než DC. Stačí vložit znak komentáře (#) před servery nastavené v `/etc/ntp.conf` (v CentOS 7 se jedná o `*.centos.pool.ntp.org`) na hodnoty serverů dc1 a dc2, přičemž preferuje se hodnota z dc1, který má být hlavním poskytovatelem AD a souvisejících služeb. Nicméně v případně výpadku je zde hodnota i z dc2.

```
server dc1.company1.local      iburst prefer

server dc2.company1.local      iburst
```

Poté lze službu spustit a získaný čas ověřit příkazem `ntpq -p`.

AD opět vyžaduje použití Kerberos. Stačí využít již existující `/etc/krb5.conf` z dc1/dc2 a například příkazem `rsync` ho přesunout na nový server (je nutné ho nainstalovat pomocí `yum install rsync` na DC i na samba1).

```
[root@samba1 ~]# rsync -a root:192.168.130.11:/etc/krb5.conf
/etc/
```

Posledním krokem je získání samotné Samby 4.7.7 a pro instalaci lze použít postup z dc1/dc2 (`wget, configure, make, make install, PATH`), přičemž jsou zde dva rozdíly.

První se týká balíčků potřebných ke kompilaci. Jelikož Samba nebude v roli doménového řadiče, ale jen člena, stačí jí zhruba polovina. Seznam je převzat z oficiálních požadavků. (Samba project, ©2018a)

```
[root@samba1 ~]# yum install autoconf automake gcc gdb krb5-
devel krb5-workstation openldap-devel make pam-devel python-
devel docbook-style-xsl libacl-devel libattr-devel libxslt
```

Druhou úpravou navazující na první je přidání parametru `--without-ad-dc` k příkazu `configure`, který neumožní Sambě stát se řadičem. Navíc by selhal v průběhu, jelikož na systému nejsou nainstalovány všechny závislosti.

Server v roli člena domény vyžaduje konfigurace souboru `smb.conf`, který se standardně nachází v `/etc/` při instalací pomocí `yum` a v `/usr/local/samba/etc/` při kompilování. Povinné parametry je možné dohledat v ukázkovém konfiguračním souboru (Samba project, ©2018l) a v mapování identit z AD (Samba project, ©2018m) na základě rfc2307 (Howard, 1998). Zde je konfigurační soubor ze samba1.company1.local, který kombinuje výše zmíněné zdroje. Hodnoty v něm je nutné upravit pro konkrétní doménu a s příslušným rozsahem přiřazovaných hodnot. Zde na doporučeném rozmezí. Ty musí následně odpovídat hodnotám `uid`/`gid` v definici objektů služby AD, jinak nedojde ke správnému překladu. Rozsah záleží na velikosti plánovaného doménového prostředí a nesmí se překrývat s žádným jiným, a to včetně systémových účtů.

Nastavení využívá zmíněné specifikace rfc2307 a také nabízí správci možnost definovat uživatelské oprávnění na základě Windows ACL místo POSIX, kterou se běžné řídí Linuxové sdílení. Zároveň je zde ukázána možnost sdílení souborů skrze Sambu pro členy domény. Ti si mohou síťovou složku připojit jako disk a plně ji využívat k práci.

```
[global]

        security = ADS

        workgroup = COMPANY1

        realm = COMPANY1.LOCAL

        log file = /var/log/samba/smblog.log

        log level = 1

        vfs objects = acl_xattr

        map acl inherit = yes

        store dos attributes = yes


        idmap config * : backend = tdb

        idmap config * : range = 3000-7999


        idmap config COMPANY1 : backend = ad

        idmap config COMPANY1 : schema_mode = rfc2307

        idmap config COMPANY1 : range = 10000-999999

        idmap config COMPANY1 : unix_primary_group = yes

        idmap config COMPANY1 : unix_nss_info = yes

[DemoShare]

        path = /firemniSoubory/

        read only = no
```

Změna nastavení pro sambu se aktivuje příkazem `smbcontrol all reload-config`. (Red Hat, Inc., ©2017 str. 268)

Nyní se server připojí do domény pomocí příkazu `net` poskytovaným Sambou a zadáním heslo administrátora.

```
[root@samba1 ~]# net ads join -U administrator
```

Aby bylo možné využívat účty definované v AD, je potřeba nakonfigurovat službu `Name Service Switch (NSS)`, respektive její soubor `/etc/nssswitch.conf`. Její funkcí je poskytovat definici pro programy o tom, kde mají hledat požadované hodnoty, například když hledají uživatele. Kupříkladu nejdřív zkontrolovat soubory (`/etc/passwd`) a poté přejít na službu `winbind`. Pro hodnoty `passwd` (získání informací o uživatelích) a `group` (o skupinách) se k danému řádku za hodnotu `files` zapíše `winbind`. Program potom dělá přesně to, co mu NSS nabízí. Nejdříve zkontroluje lokální soubory pro přihlášení uživatele/informací o skupině a poté se zeptá `winbind` na požadované údaje. Jedná se o další službu, která se zeptá AD a případně vrátí požadované hodnoty z její databáze. (Red Hat, Inc., ©2017 str. 248)

Pro správnou funkci služby `winbind` je potřeba nahrát knihovny, které Samba při `make install` nakopírovala do `/usr/local/samba/lib/`, konkrétně `libnss_winbind.so.2` do složky `lib`, respektive `/lib64` pro 64 bitový CentOS 7. Zároveň ji v téže složce zkopírovat jako `libnss_winbind.so`. Výhodnější je použít symbolický odkaz ze složky Samby, aby nebylo nutné je při aktualizace znovu kopírovat. Pro zavedení se musí restartovat server nebo spustit příkaz `ldconfig`, který knihovny zavede. (Leal, 2014 str. Configuring the PAM and NSS libraries)

V neposlední řade je konfigurace spouštěcích skriptů. Zde je vhodné se inspirovat kapitolou 9.2.6 Systemd soubory. Změna oproti řešení na DC spočívá ve využití třech takových souborů (linuxový démon `winbindd`, `smbd` a `nmbd`). Rozdíl bude spočívat v parametru `ExecStart`, kde budou postupně všechny tři vyjmenované služby (mají stejný adresář). Stejně tak změna `PIDFile` a položku `After` upravit tak, že zde `smbd` bude mít navíc `winbind.service` (respektive název vytvořeného spouštěcího skriptu pro `winbind`) a `nmbd` položku `winbind.service`

a smbd.service. Následně je stačí všechny tři aktivovat pomocí Systemctl enable a restartovat server pro test.

Využití přístupových práv dle Windows (ACL) je definováno v smb.conf na serveru samba1.company1.local. Konkrétně hodnot vfs objects, map acl inherit a store dos attributes. Aby správce mohl zadávat zmíněné ACL, musí mít on nebo příslušná skupina oprávnění SeDiskOperatorPrivilege. Operace se provede následovně. (Red Hat, Inc., ©2017 stránky 268-269)

```
[root@samba1 ~]# net rpc rights grant "COMPANY1\Domain Admins"
SeDiskOperatorPrivilege -U "COMPANY1\tomas.ruzicka"
Enter COMPANY1\tomas.ruzicka's password:
Successfully granted rights.
```

Účet tomas.ruzicka je nově definovaný pomocí aplikace Uživatelé a počítače služby Active Directory, který má korektně nastaveny všechny povinné parametry pro fungování idmap. (Red Hat, Inc., ©2017 stránky 256-257)

Nyní je možné přiřadit práva na složku za pomocí účtu z AD, přičemž se využije příkaz chown běžně dostupný v Linuxu.

```
[root@samba1 ~]# chown
„COMPANY1\\tomas.ruzicka:COMPANY1\\Domain Users“
/firemniSoubory

[root@samba1 ~]# chmod 770 /firemniSoubory
```

Ze strany serveru je konfigurace hotová. Pomocí počítače s RSAT je potřeba spustit Správa počítače a menu Akce zvolit Připojit k jinému počítači. Stačí zadat samba1.company1.local a dojde ke spojení na zmíněný server. V případě problému je vhodné problém hledat nejprve ve firewallu a DNS záznamech.

Po úspěšném připojení se vlevo nabídne sekce Správa počítače -> Sdílené složky -> Sdílené složky. Zde pod účtem s příslušnými právy lze nadefinovat klasické Windows ACL a to díky nastavení v smb.conf, které je umožní uchovávat.

Následně se definuje nová sdílená složka v rámci Active Directory za pomoci UMAC a Nový objekt -> Sdílená složka. Zadá se vhodný název a síťová cesta, tedy \\samba1.company1.local\DemoShare.

Třetím krokem je otevření Správa zásad skupiny a v rámci domény company1.local vytvořit nový objekt zásad pojmenovaný automountJ, který lze pravým tlačítkem myši editovat. Zde má správce mnohé možnosti, co a jak nastavit. Pro automatické připojení sdílené složky je ale důležitá položka Konfigurace uživatele -> Předvolby -> Nastavení systému Windows -> Mapování jednotek. Zde lze vytvořit nový příkaz pro mapování s umístěním na DemoShare, které AD nabídne. Poté mu stačí jen přiřadit písmeno „J“, zaškrtnou Znovu připojit a vhodně popsat. Tímto je provedeno základní nastavení a po přihlášení doménovým jménem se automaticky připojí disk „J“ na server samba1.

9.6.2 Využití účtů z AD pro lokální přihlášení

Systém Active Directory je vytvořený společností Microsoft. Lze předpokládat, že počítače s operačním systémem Windows s ním budou kompatibilní, i když adresářové služby poskytuje Samba. Uživatelé získají doménové přihlášení na počítači i v rámci podporovaného softwaru třetích stran. Správci mají dále možnost nastavovat síťová rozhraní, připojovat sdílené složky nebo využívat tiskárny. Ovšem nemusí se jednat jen o zásadní věci. Administrátor může například zakázat změnu pozadí a tím definovat firemní kulturu.

Z pohledu Linuxového systému nelze automaticky předpokládat, že využitím AD správce získá kompletní kontrolu i nad touto oblastí. UNIX, na kterém je Linux založen, je jiný než Windows, a proto nejdou všechny vlastnosti automaticky převést i na Linuxové stanice. I tak je částečná integrace možná. O tom se bylo možné přesvědčit při nastavení DC v kapitole 9.2 Úvodní konfigurace dc1.company1.local nebo připojením člena do domény v 9.6.1 Konfigurace.

Jaký je z toho přínos pro uživatele a administrátora? Možnost provozovat Linuxový server v režimu řadiče a poskytovat ostatním zařízením služby AD bez nutnosti nákupu licencí Windows Server. Připojit Windows stanici a využívat doménové přihlášení. Získat přístup k centrální databázi údajů. Na Linuxovém serveru

poskytovat sdílené složky pro členy domény nebo využít přihlašovacích údajů k připojení na službu SSH. Poslední možnost bude nyní představena.

V současné době fungují dc1 a dc2 jako doménové řadiče a je možné je kontaktovat pro získání uživatelů z databáze. Server samba1 toho využívá k nastavení přístupových práv na sdílených složkách, ale je zde i další možná integrace. K Linuxovému server se často přistupuje pomocí SSH protokolu. Ten poskytuje šifrované spojení a správce může na dálku ovládat konzoli vzdáleného zařízení. Standardně si služba ověřuje uživatele pomocí souboru `/etc/passwd` a `/etc/shadow`. Jedná se o lokální ověření, které zbytečně duplikuje data dostupná v AD.

Lepším způsobem je získat informace o účtech za pomoci zmíněné služby `winbind` a `PAM`. Druhá z nich představuje soubor knihoven poskytující rozhraní ostatním programům pro potřeby autentizace. Konfigurace opět zahrnuje zkopírování knihovny vytvořené Sambou a to ze složky `/usr/local/samba/lib/security/pam_winbind.so` do `/lib64/security/` a úpravy souboru `/etc/pam.d/password-auth-ac` dle doporučení Samby:

```
auth        sufficient    pam_winbind.so use_first_pass

account    [default=bad success=ok user_unknown=ignore]
pam_winbind.so

password    sufficient    pam_winbind.so use_authtok
```

(Samba project, ©2017h)

Po této úpravě je možné přihlášení na server pomocí SSH se zadáním uživatelského jména ve tvaru `user@company1.local` a hesla kde `user` představuje konkrétního uživatele z AD. Systém následně automaticky zajistí přihlášení uživatele s využitím dostupných prostředků.

V této chvíli je server samba1.company1.local zapojen jako člen domény poskytující sdílené adresáře a zároveň umožňuje i další využití uživatelských účtů ve

formě přihlášení na démona SSH. V případně problémů jej lze debugovat zastavením služby a opětovným spuštěným v nejvyšším režimu ladění (třikrát „d“).

```
[root@samba1 ~]# /usr/sbin/sshd -ddd
```

10 Ověření navrženého řešení

Po provedení všech zmíněných postupů je k dispozici funkční Active Directory provozované na platformě Linux za použití softwaru Samba. Systém splnil původní očekávání na funkčnost a po dalším testování a ověření nastavení se jeví jako velice zajímavý kandidát pro ostrý provoz. Jeho silnou stránkou je svobodná implementace, kde provozovatel není vázán licenční politikou s využitím známého a dostupného softwaru. Pádným argumentem proti jeho nasazení je problémová podpora. Oproti Microsoft řešení, který nabízí stálou technickou asistenci, je zde správce odkázán především na komunitu a dokumentaci. Obojí naštěstí funguje výborně.

Výzvou bude i samotná instalace a provoz ve firemním prostředí, jelikož standardně se pro AD využívá právě originální řešení Windows Server. Mnoho IT správců dokáže tuto platformu spravovat. Běžnou konfiguraci zvládne i ne moc zkušený jedinec, takže zádrhel může nastat až v případě vážnějších problémů. Pro interní/externí IT oddělení se nejedná o takový problém jako Linuxová alternativa.

Druhé řešení, i přes svou jednoznačně kladnou stránku v podobě open-source, představuje obrovskou výzvu. Není mnoho administrátorů, kteří by upřednostnili alternativní volbu, a to z důvodů neznalosti, vyšší technické náročnosti na instalaci i provoz a horší podporu. Nicméně při rozhodnutí jít touto cestou získá firma cenného pomocníka, který zastane velkou část komerčního řešení.

V průběhu testování byla ověřena funkčnost jak doménových řadičů, tak i případná havárie popsaná v kapitole 10.1 Řešení problémů. K systému se přidalo i sdílené uložiště distribuované skrze AD a samozřejmě možnost doménového přihlášení a zásad skupin. Technicky se jednalo o náročnou proceduru, kdy bylo potřeba mnohdy vyzkoušet různé nastavení a jeho vliv na funkčnost systému. Microsoft řešení zde má navrch v podobě přívětivého grafického rozhraní, skrze které je možné celý mechanismus řídit. Obecně je Linuxový svět méně uživatelsky přívětivý, a to především z důvodů konfigurace z příkazové řádky (shellu). Samozřejmě obsahuje i grafickou část, ale většina manuálů nebo případných uživatelských příspěvků je prováděna právě s pomocí příkazové řádky. Navíc když si na něj správce zvykne, tak zjistí, že nabízí možnost velmi rychlého nastavení systému, přehledu o jeho stavu a jednotnou cestu, jak provést určitou konfiguraci.

10.1 Řešení problémů

10.1.1 Porucha dc1.company1.local

V průběhu vytváření serveru samba1.company1.local bylo potřeba instalaci Samby odstranit a znovu ji nakonfigurovat. Ke smazání byl použit příkaz

```
[root@dc1 ~]# rm -Rf /usr/local/samba
```

který má za úkol provést rekurzivní odstranění všech souborů v zadané cestě (-R) a má být vynucené, aby uživatel nebyl dotazován, zda chce soubor skutečně smazat (-f). Tento příkaz byl omylem použit na jiném serveru, a to na doménovém řadiči dc1, který zároveň obstarával všechny FSMO role.

V tu chvíli zareagoval druhý doménový řadič a dle očekávání pokračoval v poskytování AD služeb. Samozřejmě nemohl kontaktovat dc1, a proto začal vypisovat chyby, že se nelze na dané zařízení připojit a replikace má neplatné pokusy.

```
[root@dc2 ~]# samba-tool drs showrepl
```

Bylo nutné rychle obnovit provoz FSMO rolí. Bohužel původní řadič byl zcela mimo provoz (ekvivalent kompletní HW poruchy), takže nebylo možné řádně přesunout veškeré role. Místo toho došlo k násilnému převzetí příkazem z dc2.

```
[root@dc2 ~]# samba-tool fsmo seize --role=all
```

Ten z něj udělal držitele všech FSMO rolí. Pokud by se podařilo obnovit dc1 (což zde nebylo možné), tak po převzetí rolí se nesmí opět připojit do AD, jinak dojde k narušení databáze a systém se stane nestabilním. Bohužel výsledek nedopadl dle očekávání a nastala chyba při pokusu o přesun `DOMAINDNS` a `FORESTDNS`.

```
Failed to connect to ldap URL 'ldap://ee022ddd-52e2-41bb-
bf73-25219862f627._msdcs.company1.local' - LDAP client
internal error: NT_STATUS_CONNECTION_REFUSED
```

Při druhém pokusu stejná chyba nevznikla a dc2 hlásil úspěšně převzetí `DOMAINDNS`. Nicméně při pokusu o přesun `FORESTDNS` se situace opakovala a opět byl přesun dokončen s chybou. Stav rolí se ověřil následujícím příkazem.

```
[root@dc2 ~]# samba-tool fsmo show
```

Systém hlásil úspěšné přesunutí, ale chybové hlášky tomuto výsledku na důvěře nepřidaly. V rámci testovacího provozu bylo rozhodnuto s přesunem pokračovat a původní řadič zcela odstranit.

```
[root@dc2 ~]# samba-tool domain demote --remove-other-dead-
server=dc1
```

Po obnově dc1 pomocí nové instalace Samby a připojením do domény byl proveden pokus o přesun FSMO rolí. Původní konfigurace byla smazána a mělo by tedy být možné ho opět připojit do domény.

```
[root@dc1 ~]# samba-tool fsmo transfer --role=all
```

Přesun `RID` serveru proběhl úspěšně, ale následně při přesunu `PDC` došlo k vypršení exekučního času pro příkaz.

```
ERROR: Transfer of 'pdc' role failed: Failed FSMO transfer:
NT_STATUS_IO_TIMEOUT
```

Na první pohled se systém tvářil tak, že RID server je na dc1 a zbytek na dc2. Pro ověření byl použit příkaz s dotazem na rozmístění FSMO funkcí.

```
[root@dc1 ~]# samba-tool fsmo show
```

Výsledek ukázal, že dc1 drží nejen `RID`, ale i `PDC`, čemuž neodpovídala minulá chybová hláška s překročením časového plánu při přesunu `PDC`. I přes podivné chování se pokračovalo v přesunech a povedlo se vše, až na `DOMAINDNS` a `FORESTDNS`. Ty skončily s následující chybou (případně `DC=ForestDnsZones` u `FORESTDNS` FSMO).

```
ERROR: Failed to delete role 'domaindns': LDAP error 50
LDAP_INSUFFICIENT_ACCESS_RIGHTS -  <00002098: Object
CN=Infrastructure,DC=DomainDnsZones,DC=company1,DC=local has
no write property access> <>
```

To bylo možné vyřešit definováním uživatele pro danou akci parametrem -U.

```
[root@dc1 ~]# samba-tool fsmo transfer --role=domaindns -U
administrator
```

Nicméně i ta po zadání hesla skončila chybovou hláškou na neexistující atribut `drs_utils`. Zpráva je pro potřeby této práce zkrácena.

```
ERROR(<type 'exceptions.AttributeError'>): uncaught exception
- 'module' object has no attribute 'drs_utils'

…

except samba.drs_utils.drsException, e:
```

Následný dotaz na stav FSMO rolí proběhl úspěšně a systém hlásil, že je vše v pořádku. Převzetí/přesun rolí byl tedy dokončen, ale s mnoha problémy. Po zásahu se veškeré použité funkce zdály být funkční, ale při produkčním nasazení je potřeba mít 100 % jistotu v přesunu. Chyba mohla způsobit nekonzistenci dat v databázi nebo jiné problémy, které nebyly na první pohled zřetelné.

Po dané zkušenosti klesla důvěra v použitý software. Samozřejmě, jednalo se o velice nešťastnou chybu, kdy se smazání Samby dalo předejít důslednější kontrolou připojeného serveru, ale principiálně stejný problém nastane při HW poruše.

Program pro tyto a jim podobné situace sice obsahuje možnosti, jak krizi zvládnout, nicméně dle výše popsané zkušenosti nefungují zcela spolehlivě. Následně možné problémy mohou mít fatální důsledky pro celou organizaci a její uživatele. Případná nekonzistence dat nebo jiná chyba se může projevit až časem a velice ztížit její nápravu.

10.1.2 Chyba při aktualizaci DNS záznamů

Vytvoření domény na dc1 proběhlo v pořádku a po dokončení zbylého nastavení se rovnou přešlo k nastavení dc2. Připojení do company1.local pomocí `samba-tool domain join` proběhlo také v pořádku (tedy za předpokladu, že se nezapomnělo smazat soubor `/etc/krb5.conf`). Bylo možné ověřit i rozložení FSMO rolí

```
[root@dc2 ~]# samba-tool fsmo show
```

a stav replikace.

```
[root@dc2 ~]# samba-tool drs showrepl
```

Vše se tvářilo v pořádku a po dalších testech byl připojen server samba1.company1.local sloužící jako poskytoval sdíleného prostoru. Tady ale nastal další problém. Pomocí příkazu `net` byl zadán požadavek na připojení do domény, který ale neskončil zcela úspěšně.

```
[root@samba1 ~]# net ads join -U administrator

Enter administrator's password:

Using short domain name -- COMPANY1

Joined 'SAMBA1' to dns domain 'company1.local'

DNS Update for samba1.company1.local failed:
ERROR_DNS_UPDATE_FAILED

DNS update failed: NT_STATUS_UNSUCCESSFUL
```

Výsledek programu zahlásil připojení do domény, ale také chybu při aktualizaci DNS. Vyhledáním chybové hlášky bylo zjištěno, že problém bude nutné hledat na straně doménových řadičů. To postupně vedlo až k testování dynamických DNS aktualizací, kde byla zjištěna chyba. Test lze provést následovně na obou DC.

```
[root@dc1 ~]# samba_dnsupdate --all-names
```

Ten zkontroluje chybějící záznamy v `/usr/local/samba/private/dns_update_list`. Procedura proběhla na dc1 v pořádku, ale dc2 vykazoval problém například na následujícím záznamu.

```
Failed nsupdate: 1

update(nsupdate): A DomainDnsZones.company1.local
192.168.130.11

Calling nsupdate for A DomainDnsZones.company1.local
192.168.130.11 (add)

Successfully obtained Kerberos ticket to
DNS/dc1.company1.local as DC2$

Outgoing update query:

;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0

;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0

;; UPDATE SECTION:

DomainDnsZones.company1.local. 900 IN   A
192.168.130.11

dns_tkey_negotiategss: TKEY is unacceptable
```

Ve výsledku selhala aktualizace všech dotazů.

```
Failed nsupdate: 1

Failed update of 28 entries
```

Zmíněné chybě se také věnuje následující odkaz. (Samba project, ©2017f)

Bylo zjištěno, že na dc2 chyběl záznam `dns-DC1`. Bohužel standardní rekonfigurace pomocí `samba_upgradedns --dns-backend=BIND9_DLZ` nezafungovala a bylo nutné aktivovat nejvyšší stupeň logování softwaru Samba a zkoumat příčinu problému. Ze záznamu bylo patrné, že server dc2 dostal i Kerberos ticket od dc1, ale z nějakého důvodu neproběhla aktualizace údajů.

Zkoumání bylo velmi dlouhé a náročné. Vyzkoušeno bylo i odebrání záznamu o účtu `dns-DC2`, rekonfigurace na `SAMBA_INTERNAL` a zpátky na `BIND9_DLZ`,

nastavování služby BIND, odebrání `dns.keytab` a jeho vytvoření, ale i vynucená replikace AD ze strany dc1.

```
[root@dc1 ~]# samba-tool drs replicate dc2 dc1
dc=company1,dc=local --full-sync
```

Synchronizace AD napříč DC společně s `samba_upgradedns --dns-backend=BIND9_DLZ` doplnila odebrané záznamy `dns-DC1` a `dns-DC2`. To ale problém neopravilo.

Během testování se chvílema podařilo získat kladný výsledek ze `samba_dnsupdate` (tedy bez chyby `TKEY`), kdy se dc2 tvářil, že hodnoty jsou v pořádku. Po určité době/restartu serveru se ale daná chyba opět vrátila, což bylo ještě podivnější a nepřidávalo systému na důvěryhodnosti pro ostrý provoz.

Finální řešení přinesla až konfigurace `resolv.conf`, která byla inspirována emailovou konverzací se Samba týmem (Hunter, a další, 2016), a na jejím základě došlo ke zrušení dvou hodnot ve zmíněném souboru (symbol # udělá z textu poznámku a program jej ignoruje) a doplnění jedné nové.

```
#nameserver 192.168.130.10    #dc1

#nameserver 192.168.130.11    #dc2

 nameserver 127.0.0.1
```

Po této úpravě, která byla následně provedena i na dc1, systém nevracel žádnou chybovou hlášku a veškeré údaje se zdály být v pořádku. Fungovala i replikace, FSMO role, služba Kerberos i DNS. Důvod, proč musela mít položka `nameserver` hodnotu 127.0.0.1 (adresa zvaná `localhost` označující to zařízení, na kterém se soubor nachází) a ne přímo IP adresu toho stejného serveru není známa a nepodařilo se ji ani dohledat.

11 Vyhodnocení hypotéz

Myšlenkou celého řešení bylo poskytnout služby Active Directory na systému CentOS 7. Toto snažení bylo v konečném důsledku úspěšné, i když technicky mnohem náročnější než při využití originálního produktu Windows Server, a to jak z hlediska nasazení, tak budoucí údržby a upgradu. Konečným záměrem je se vyhnout komerčnímu řešení, kde je potřeba řešit licenční politiku a místo toho využít open-source programy, tedy s otevřeným kódem pro případnou revizi/modifikaci.

Hypotézy na sebe postupně navazují. Nejdříve je potřeba uživateli nabídnout doménové funkce, ale s předpokladem vysoké dostupnosti. Následně ověřit, že se může přihlásit do testovacího prostředí a na závěr že mu správcem mohou být distribuovány objekty skupinové politiky.

Hypotéza 1 - Funkce poskytované doménovým řadičem budou provozovány v režimu vysoké dostupnosti. Porucha jednoho tedy neohrozí fungování zbytku sítě.

Tato hypotéza byla potvrzena v kapitole 9.2 Úvodní konfigurace dc1.company1.local, 9.3 Úvodní konfigurace dc2.company1.local a 9.4 Replikace. Nejprve byl vytvořen doménový řadič dc1 a následně se k němu přidal i dc2. Mezi nimi probíhaly automatické replikace v multi-master režimu a jeden ze serverů obstarával všechny FSMO role. Nechtěně bylo vyzkoušeno i násilné převzetí všech rolí řadičem dc2 po fatální chybě, kdy došlo ke smazání složky na špatném serveru.

Replikace databáze AD fungovala výborně, ale v rámci HA je potřeba ručně vyřešit i synchronizace adresáře Sysvol, který není v Samba multi-master režimu podporován.

Hypotéza 2 - Doménový řadič umožní připojení a přihlášení klientského PC s Windows 10 Pro 64 bit a CentOS 7 64 bit do domény.

Nasazením doménových řadičů začalo fungovat doménové prostředí s názvem company1.local. Následně se připojil další Linuxový server se Sambou, ale tentokrát z důvodů poskytování sdílení v rámci AD. Bylo tedy nutné vyřešit jeho začlenění do domény, čemuž se věnuje kapitola 9.6 Souborový server. Tím byla vyřešena polovina

úkolu za OS Linux v rámci hypotézy 2. Přihlášení s využitím doménových údajů se věnuje kapitola 9.6.2 Využití účtů z AD pro lokální přihlášení.

Ze strany Windows stanice bylo ověřeno opět jak připojení, tak přihlášení uživatele, a navíc i využití nástroje RSAT pro správu AD 9.5 Připojení Windows stanice.

Hypotéza 2 se ukázala pravdivá.

Hypotéza 3 - Počítače s OS Windows budou využívat doménové politiky nastavené správcem, jako je například automatické připojení síťového disku.

Posledním předpokladem bylo možnost využít skupinových zásad pro distribuci nastavení na Windows počítače. Originální AD má sílu právě ve vytvoření, centrální správě a snadné aplikaci zmíněných zásad. Testování ukázalo, že pro řešení Samba lze využít RSAT nástroje od Microsoft, které dokáží ovládat AD a je zde podporována standardní správa politiky. V rámci ověření funkčnosti bylo nastaveno automatické mapování síťové složky jako disk „J“, který se uživatelům po řádném přihlášení sám připojil a nabídnul požadovaná data.

Poslední z hypotéz byla taktéž potvrzena a prokázána jako funkční.

12 Závěr

Cílem diplomové práce bylo zmapovat open-source řešení CentOS 7 a softwaru Samba 4 pro využití jako základní platformy poskytující adresářové služby.

V rámci implementace na alternativním systému bylo potřeba popsat teoretické principy původního Active Directory. Nejprve byl čtenář seznámen se základní strukturou a jejími součástmi zahrnující les, strom, doménu a organizační jednotky. Dozvěděl se, jaká je mezi nimi souvislost, aby je mohl použít při návrhu nového řešení.

Poté se popis přesunul k DNS sloužící k překladu doménových jmen na IP adresy, které představuje klíčový prvek potřebný k provozu.

Před realizací praktické části se práce věnuje otázce bezpečnosti a s tím související vztahy důvěry, které dávají nebo zakazují uživatelům možnost získat informace z jiné domény, a autentizačnímu mechanismu Kerberos pro šifrované ověření v nezabezpečených sítích.

Opomenuta není ani problematika FSMO rolí, které rozdělují vybrané úkony mezi servery a téma nasazení adresářových služeb v korporátních sítích včetně manažeru identit.

Po zkoumání a následné realizaci navrhnutého řešení byl systém spuštěn a úspěšně potvrdil všechny tři stanovené hypotézy. První z nich ověřovala, zda systém umí poskytnout potřebné funkce v režimu vysoké dostupnosti. Druhá se zaměřila na uživatele a bylo potřeba potvrdit, zda nově vytvořený systém umožní připojení Windows 10 a CentOS 7 do domény. Třetí rozšiřovala nabízené možnosti a zkoumala využití doménové politiky řízené správcem na začleněná Windows PC s možností automatického připojení síťového disku. Hypotézy měly prokázat funkčnost vytvořeného systému a potvrdit, že ho lze využít ve firemní sféře v heterogenních sítích.

Ukázalo se, že Samba 4 s Linuxovým základem nabízí pro tyto účely dostatečnou funkcionalitu, kterému by ale i tak měla předcházet důkladná fáze testování. Oproti komerčnímu řešení Active Directory zde není nutné řešit nákup drahých licencí, a to díky výběru open-source softwaru. Nevýhodou je neoficiální podpora, kterou lze alespoň částečně kompenzovat využitím OS RHEL od společnosti Red Hat.

Navržené řešení v této práci navíc využívá komponent, které jsou neustále aktualizovány a postupně integrují další mechanismy. Z toho důvodu bude systém i nadále testován, rozšiřován a postupně bude využít pro reálné použití. Plánovaná je integrace s bezpečnostním řešením Kerio Control od společnosti GFI, dále emailového řešení Kerio Connect a další vhodné aplikace, které podporují propojení s AD. Veškeré tyto akce jsou již plně v režii správce systému, který se musí postarat o vhodné propojení.

Celkově lze tuto kombinaci doporučit jako alternativu k Microsoft prostředí, kdy není nutné spoléhat na jediné řešení. Zahrnuje to ale náročnější nasazení i provoz a obecně vyšší nároky na IT správce. Zajímavou volbou může být i zmíněný Zentyal, které poskytne adresářové služby jako kompaktní systém a přívětivým GUI.

13 Citovaná literatura

Hannifin, Dustin, Alpern, Naomi J. a Alpern, Joey. 2010. *Microsoft Windows Server 2008 R2.* 1. místo neznámé : Elsevier, 2010. 978-1-59749-578-3.

Howard, L. 1998. An Approach for Using LDAP as a Network Information Service. [Online] Březen 1998. [Citace: 2. Červen 2018.] https://www.rfc-editor.org/rfc/rfc2307.txt.

Hunter, Jonathan a Louis. 2016. [Samba] drs showrepl - Failed to bind to UUID - Undetermined error. [Online] 9. Září 2016. [Citace: 9. Červen 2018.] https://lists.samba.org/archive/samba/2016-September/202780.html.

Jose, Dieguez Castro. 2016. *Introducing Linux Distros.* 1. Berkeley : Apress, 2016. 978-1-4842-1392-6.

Leal, Marcelo. 2014. *Implementing Samba 4.* Livery Place : Packt Publishing Ltd., 2014. str. 473. 978-1-78216-658-0.

Microsoft Corporation. ©2014b. Active Directory FSMO roles in Windows. [Online] 23. Duben ©2014b. [Citace: 4. Červen 2018.] https://support.microsoft.com/cs-cz/help/197132/active-directory-fsmo-roles-in-windows.

—. ©2012. Basic Concepts for the Kerberos Protocol. [Online] 18. Červenec ©2012. [Citace: 21. Březen 2018.] https://technet.microsoft.com/en-us/library/cc961976.aspx.

—. ©2018a. Best Practices for Sysvol Maintenance. [Online] 17. Duben ©2018a. [Citace: 8. Květen 2018.] https://support.microsoft.com/en-us/help/324175/best-practices-for-sysvol-maintenance.

—. ©2017b. Comparison of Standard and Datacenter editions of Windows Server 2016. [Online] 3. Leden ©2017b. [Citace: 3. Květen 2018.] https://docs.microsoft.com/en-us/windows-server/get-started/2016-edition-comparison.

—. ©2018d. FSMO placement and optimization on Active Directory domain controllers. [Online] 17. Duben ©2018d. [Citace: 4. Červen 2018.] https://support.microsoft.com/en-ca/help/223346/fsmo-placement-and-optimization-on-active-directory-domain-controllers.

—. ©2018c. Identity and Access in Windows Server 2016. *Identity and Access | Microsoft Docs.* [Online] 16. Březen ©2018c. [Citace: 24. Duben 2018.] https://docs.microsoft.com/en-us/windows-server/opbuildpdf/identity/TOC.pdf?branch=live.

—. ©2018b. Licencování a ceny pro Windows Server 2016. [Online] ©2018b. [Citace: 29. Duben 2018.] https://www.microsoft.com/cs-cz/cloud-platform/windows-server-pricing.

—. ©2017a. Remote Server Administration Tools. [Online] 17. Březen ©2017a. [Citace: 1. Květen 2018.] https://docs.microsoft.com/en-us/windows-server/remote/remote-server-administration-tools.

—. ©2018e. Remote Server Administration Tools (RSAT) for Windows operating systems. [Online] 17. Duben ©2018e. [Citace: 11. Červen 2018.] https://support.microsoft.com/en-us/help/2693643/remote-server-administration-tools-rsat-for-windows-operating-systems.

—. ©2009. Trust Technologies: Domain and Forest Trusts. [Online] 8. Říjen ©2009. [Citace: 31. Leden 2018.] https://msdn.microsoft.com/en-us/library/cc759554(v=ws.10).aspx?f=255&MSPPError=-2147217396.

—. ©2012. Understanding Trusts | Microsoft Docs. [Online] 3. Července ©2012. [Citace: 31. Leden 2018.] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731335%28v%3dws.10%29.

—. ©2014a. What Are Domains and Forests? [Online] 19. Listopad ©2014a. [Citace: 5.. 1. 2018.] https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx.

Rahman, Habibar. 2014. DNS Records that are required for proper functionality of Active Directory. [Online] 12. Červenec 2014. [Citace: 11. Červen 2018.] https://blogs.msdn.microsoft.com/servergeeks/2014/07/12/dns-records-that-are-required-for-proper-functionality-of-active-directory/.

Red Hat, Inc. ©2017. System Administrator's Guide. [Online] ©2017. [Citace: 30.. 11. 2017.] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/index.

Ricciardi, Fulvio. 2007. MIT Kerberos Consortium - Protocol Tutorial. *MIT Kerberos Consortium.* [Online] 1.0.3, 27. Listopad 2007. [Citace: 21. Březen 2018.] https://www.kerberos.org/software/tutorial.html.

Samba project. ©2017h. Authenticating Domain Users Using PAM. [Online] 26. Únor ©2017h. [Citace: 12. Červen 2018.] https://wiki.samba.org/index.php/Authenticating_Domain_Users_Using_PAM.

—. ©2018h. BIND9 DLZ DNS Back End. [Online] 29. Leden ©2018h. [Citace: 4. Červen 2018.] https://wiki.samba.org/index.php/BIND9_DLZ_DNS_Back_End.

—. ©2017f. Dns tkey negotiategss: TKEY is unacceptable. [Online] 26. Únor ©2017f. [Citace: 9. Červen 2018.] https://wiki.samba.org/index.php/Dns_tkey_negotiategss:_TKEY_is_unacceptable.

—. ©2018k. FAQ. [Online] 26. Květen ©2018k. [Citace: 6. Červen 2018.] https://wiki.samba.org/index.php/FAQ#Is_Samba_as_an_Active_Directory_Domain_Controller_Stable_Enough_for_an_Production_Environment.3F.

—. ©2017c. Flexible Single-Master Operations (FSMO) Roles. [Online] 7. Červen ©2017c. [Citace: 4. Červen 2018.] https://wiki.samba.org/index.php/Flexible_Single-Master_Operations_(FSMO)_Roles#The_seven_FSMO_roles.

—. ©2018m. Idmap config ad. [Online] 18. Únor ©2018m. [Citace: 10. Červen 2018.] https://wiki.samba.org/index.php/Idmap_config_ad.

—. ©2018i. Joining a Samba DC to an Existing Active Directory. [Online] 18. Duben ©2018i. [Citace: 5. Červen 2018.] https://wiki.samba.org/index.php/Joining_a_Samba_DC_to_an_Existing_Active_Directory.

—. ©2017d. Managing the Samba AD DC Service Using Systemd. [Online] 6. Listopad ©2017d. [Citace: 5. červen 2018.] https://wiki.samba.org/index.php/Managing_the_Samba_AD_DC_Service_Using_Systemd.

—. ©2018a. Package Dependencies Required to Build Samba. [Online] 9. Květen ©2018a. [Citace: 12. Květen 2018.] https://wiki.samba.org/index.php/Package_Dependencies_Required_to_Build_Samba.

—. ©2017e. Raising the Functional Levels. [Online] 19. Prosinec ©2017e. [Citace: 8. Červen 2018.] https://wiki.samba.org/index.php/Raising_the_Functional_Levels#Supported_Functional_Levels.

—. ©2017a. Running a Samba AD DC with MIT Kerberos KDC. [Online] 9. Srpen ©2017a. [Citace: 12. Květen 2018.] https://wiki.samba.org/index.php/Running_a_Samba_AD_DC_with_MIT_Kerberos_KDC.

—. ©2018j. Samba 4.7.7 Available for Download. [Online] 17. duben ©2018j. [Citace: 5. červen 2018.] https://www.samba.org/samba/history/samba-4.7.7.html.

—. ©2018d. Samba AD DC Port Usage. [Online] 31. Květen ©2018d. [Citace: 2. Červen 2018.] https://wiki.samba.org/index.php/Samba_AD_DC_Port_Usage.

—. ©2017g. Samba Domain Member Port Usage. [Online] 26. Únor ©2017g. [Citace: 11. Červen 2018.] https://wiki.samba.org/index.php/Samba_Domain_Member_Port_Usage.

—. ©2018g. Setting up a BIND DNS Server. [Online] 2. Leden ©2018g. [Citace: 4. Červen 2018.] https://wiki.samba.org/index.php/Setting_up_a_BIND_DNS_Server.

—. ©2018e. Setting up RFC2307 in AD. [Online] 27. Duben ©2018e. [Citace: 2. Červen 2018.] https://wiki.samba.org/index.php/Setting_up_RFC2307_in_AD.

—. ©2018l. Setting up Samba as a Domain Member. [Online] 4. Červen ©2018l. [Citace: 6. Červen 2018.] https://wiki.samba.org/index.php/Setting_up_Samba_as_a_Domain_Member.

—. ©2018c. Setting up Samba as an Active Directory Domain Controller. [Online] 18. Duben ©2018c. [Citace: 2. Červen 2018.] https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller.

—. ©2017b. SysVol replication (DFS-R). [Online] 26. Únor ©2017b. [Citace: 12. Květen 2018.] https://wiki.samba.org/index.php/SysVol_replication_(DFS-R).

—. ©2018f. The Samba AD DNS Back Ends. [Online] 10. Květen ©2018f. [Citace: 2. Červen 2018.] https://wiki.samba.org/index.php/The_Samba_AD_DNS_Back_Ends.

—. ©2018b. Time Synchronisation. [Online] 26. Duben ©2018b. [Citace: 2. Červen 2018.] https://wiki.samba.org/index.php/Time_Synchronisation.

Smith, William a Edge Jr., Charles S. 2015. *Enterprise Mac Administrator's Guide.* 2. Berkeley : Apress, 2015. 978-1-4842-1706-1.

Stanek, William R. 2009. *Active Directory: Kapesní rádce administrátora.* 1. Brno : Computer Press, a.s., 2009. 978-80-251-2555-7.

The CentOS Project. ©2017. About CentOS. [Online] ©2017. [Citace: 5. 12 2017.] https://www.centos.org/about/.

Univention GmbH. ©2017. Manual for users and administrators. [Online] ©2017. [Citace: 18.. 12. 2017.] https://docs.software-univention.de/manual-4.2.html.

Whitt, Phillip. 2015. *Pro Freeware and Open Source Solutions for Business.* 1. Berkeley : Apress, 2015. 978-1-4842-1130-4.

Zentyal S.L. ©2017. En/5.0/Zentyal 5.0 Official Documentation. [Online] 18.. 4. ©2017. [Citace: 15.. 12. 2017.] https://wiki.zentyal.org/wiki/En/5.0/Zentyal_5.0_Official_Documentation.