Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Souborový server na operačním systému Linux

Jan Cinybulk

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Cinybulk

Informatika

Název práce

Souborový server na operačním systému Linux

Název anglicky

Fileserver on Linux operating system

Cíle práce

Cílem této práce je nainstalovat a nakonfigurovat souborový server na operačním systému Linux, aby byl použitelný v rámci firemní domény Active Directory. Souborový server bude umožňovat udělení přístupů jednotlivým uživatelům a skupinám z Active Directory.

Metodika

V rámci teoretické části práce bude popsána technologie Samba a adresářová služba Active Directory. V praktické části práce práce bude provedena instalace vhodné Linuxové distribuce a konfigurace programu Samba. Poté bude server zařazen do domény a nastaveny jednotlivé sdílené složky, k tomuto bude využita protokol SMB, který umožňuje fungování Linuxového serveru v doméně Active directory. Nakonec bude ověřena funkčnost sdílených složek a zabezpečení pomocí uživatelských účtů v doméně.

Doporučený rozsah práce

30-40 stran

Klíčová slova

souborový server, fileserver, Linux, SMB, Samba, Active Directory

---

Doporučené zdroje informací

BARRETT, Daniel J. Linux pocket guide. 3rd edition. Beijing: O'Reilly, 2016. ISBN 978-1491927571.
CARTER, Gerald, Jay TS a Robert ECKSTEIN. Using Samba. 3rd ed. Beijing: O'Reilly, c2007. ISBN 978-0596007690.
NEGUS, Christoper. Linux Bible. 10th Edition. Wiley, 2020. ISBN 978-1119578888.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 28. 11. 2023

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 9. 2. 2024

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 11. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Souborový server na operačním systému Linux" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2024 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Markovi Píckovi, Ph.D. za pomoc a odborné vedení, při zpracování této bakalářské práce.

Souborový server na operačním systému Linux

Abstrakt

Tato bakalářská práce se zabývá instalací a konfigurací souborového serveru v doméně Active Directory na operačním systému Linux.

V teoretické části jsou popsány technologie, kterých využívá souborový server jak z hlediska hardwaru, tak z hlediska softwaru a síťové komunikace. Dále je zde popsána doména Active Directory a technologie, kterých Active Directory využívá pro své fungování.

V praktické části je provedena konfigurace diskového pole RAID. Dále je provedena instalace operačního systému Linux v distribuci Ubuntu LTS 22.04 a je provedeno základní nastavení. Následně jsou nainstalovány potřebné softwarové balíčky, server je připraven pro zařazení do domény Active Directory a toto zařazení je provedeno. Poté jsou nakonfigurovány sdílené složky a přístupová práva doménových uživatelů a skupin. Nakonec jsou tato práva k přístupu otestována.

Klíčová slova: souborový server, Linux, Ubuntu, SMB, Samba, Active Directory, konfigurace souborového serveru, počítačové sítě

Fileserver on Linux operating system

Abstract

This bachelor thesis deals with the installation and configuration of a file server in an Active Directory domain on a Linux operating system.

The theoretical part describes the technologies used by the file server in terms of hardware, software, and network communication. It also describes the Active Directory domain and the technologies that Active Directory uses to function.

In the practical part, the configuration of a RAID disk array is performed. Furthermore, the installation of the Linux operating system in the Ubuntu LTS 22.04 distribution is performed and the basic setup is done. Then the necessary software packages are installed, the server is prepared for joining the Active Directory domain and this joining is performed. The shared folders and access rights of domain users and groups are then configured. Finally, these access rights are tested.

Keywords: fileserver, Linux, Ubuntu, SMB, Samba, Active Directory, fileserver configuration, computer networks

Obsah

1 Úvod

Souborové servery patří k nejzákladnějším typům serverů a používá je drtivá většina firem. Využívají se převážně ke sdílení souborů mezi uživateli, přenosu souborů uživatele mezi pracovními stanicemi, k odkládání souborů, které na pracovní stanici uživatele zabírají velké množství prostoru, nebo ke zprostředkování nutných souborů pro některý software. Dalo by se říct, že většina firem by dnes již bez přítomnosti souborových serverů v síti nemohla vůbec fungovat.

Při používání souborového serveru je někdy žádoucí omezit přístup k souboru pouze pro určité osoby, nebo skupiny osob. K tomuto ve firmách slouží doména Active Directory, která drží informace o všech uživatelích a jejich skupinách a zprostředkovává jejich autentifikaci. Přes Active Directory funguje samotné přihlašování do systému Windows, a proto se tato služba používá i pro určování oprávnění přístupů ke složkám a souborům.

Cílem této bakalářské práce je instalace a konfigurace souborového serveru pro použití v síti velkého rozsahu. K tomuto je použit operační systém Linux v kombinaci se softwarovým balíčkem Samba.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce bylo nainstalovat operační systém Linux a vhodnou sadu aplikačních balíčků pro fileserver a následně systém a aplikace nakonfigurovat a zařadit do existující firemní domény Active Directory. Server musí umožnit přístup pouze doménovým uživatelům. Výsledkem práce je funkční a stabilní souborový server ve firemní doméně, který bude nasazen v síti Obvodního soudu pro Prahu 1.

2.2 Metodika

Jako první je nutné vybrat vhodnou distribuci operačního systému Linux. Jako hlavní kritéria byla zvolena orientace distribuce na servery, stabilita, dostupnost a nezastaralost potřebných softwarových balíčků v repozitářích a kvalita dokumentace. Na základě těchto kritérií byla vybrána distribuce Ubuntu, která poskytuje dobrý kompromis mezi častými aktualizacemi a stabilitou a v repozitářích má všechny balíčky potřebné pro potřeby této práce.

Před instalací operačního systému budou pevné disky serveru spojeny do diskového pole RAID. Následně bude nainstalován operační systém Linux. Operační systém bude nakonfigurován pro fungování v síti. Poté budou nainstalovány balíčky pro zařazení serveru do domény a sdílení složek. Na serveru bude nastavena synchronizace systémového času protokolem NTP, server bude zařazen do domény pomocí utility realmd prostřednictvím balíčku winbind a toto zařazení bude otestováno. Nakonec budou nakonfigurovány sdílené složky v softwaru samba a oprávnění k přístupu uživatelů z Active Directory. Bude proveden test funkčnosti sdílených složek a řízení přístupů.

3 Teoretická východiska

3.1 Diskové pole RAID

Požadavky na velikost úložiště neustále narůstají, a tak se skoro každá firma dostane do situace, kdy už jí nestačí dostupné kapacity jednotlivých pevných disků a nastane potřeba využívat více pevných disků naráz. Nejjednodušší metodou pro zpřístupnění více disků naráz je disky nechat zvlášť, jako samostatné jednotky. To je ale uživatelsky nepřívětivé, jelikož se uživatel musí vždy rozhodnout na který disk data uloží. Navíc to komplikuje vyhledávání již uložených souborů, pokud jsou data na discích rozházeny nesystematicky. Ke sloučení více disků se používá diskové pole RAID neboli vícenásobné pole nezávislých disků (Šulc, 2008).

3.1.1 Hardwarový a softwarový RAID

Po technické stránce se RAID dělí na hardwarový a softwarový podle toho, jestli se o správu a čtení a ukládání dat stará dedikovaný RAID řadič a disky jsou tedy připojeny do tohoto řadiče, nebo jestli jsou disky připojeny standartně do základní desky a RAID pole je ve správě softwaru běžícího pod operačním systémem.

Hardwarový RAID se využívá u většiny serverů. Potřebný řadič může být integrovaný přímo na základní desce serveru, nebo je přítomen na rozšiřující PCI-e kartě. RAID řadič má svůj vlastní procesor a operační paměť, které jsou nezávislé na procesoru a operační paměti hostitelského stroje. Konfigurace hardwarového pole RAID se provádí ve speciálním prostředí, do kterého se lze dostat v momentě, kdy BIOS inicializuje zařízení, tedy ještě předtím, než započne zavádění operačního systému. Mezi hlavní výhody hardwarového RAID pole patří hlavně rychlost, jelikož práci s polem obstarává řadič, z hlediska vytížení procesoru není práce s daty v RAID poli o nic náročnější než s daty na disku. Další výhodou je nezávislost na operačním systému, kdy v případě selhání operačního systému nedojde k poškození pole a s daty uloženými v poli lze nadále nakládat. Hlavní nevýhodou je vysoká cena, kvůli nutnosti zakoupení dedikovaného RAID řadiče, který většinou bývá velmi nákladný. (Microsemi, 2017).

Softwarový RAID se nejčastěji využívá v podobě jednoduchého zrcadlení, nebo prokládání, a na místech, kde je kladen důraz na dostupnost dat. U softwarového RAID pole se nedoporučuje využívat komplexnější RAID algoritmy, protože více vytěžují procesor a můžou celý stroj zpomalit až za hranici použitelnosti. Na rozdíl od hardwarové varianty

nelze ze softwarového RAID pole bootovat operační systém, jelikož k datům v softwarovém poli lze přistupovat až prostřednictvím služeb, které běží jako součást operačního systému (Microsemi, 2017).

3.1.2 Jednoduché typy RAID polí

JBOD

U diskového pole typu JBOD není jasný konsenzus, jestli jej lze vůbec řadit mezi RAID pole, protože u něj nedochází k žádným speciálním operacím s daty. V poli JBOD jsou disky zřetězeny za sebe a zaplňují se postupně jeden po druhém. Velikost pole je tedy rovna součtu velikostí všech zapojených disků. Mezi výhody tohoto pole patří hlavně jednoduchost rozšíření kapacity, kdy stačí zapojit jakýkoliv disk a jeho kapacita se automaticky přičte k celkové kapacitě pole. V případě selhání jednoho z disků jsou všechna data na daném disku nenávratně ztracena, jelikož v poli JBOD nedochází k jakýmkoli výpočtům parity dat.

RAID 0

Diskové pole RAID 0 funguje na principu prokládání dat, kdy zapisovaná data jsou rozdělena na počet stejně velkých dílů rovný počtu dostupných disků a tyto díly jsou rovnoměrně zapsány na disky. V případě zapojení stejně velkých disků je dostupná kapacita pole rovná součtu velikostí všech dostupných disků. U různě velkých disků je dostupná kapacita rovna násobku počtu disků a velikosti nejmenšího disku. Nevyužitou kapacitu disků nelze jinak využít. V případě poškození jednoho z disků jsou většinou všechna data v poli ztracena, jelikož části dat jsou rovnoměrně rozděleny na všech discích a všechny disky jsou tak kritické pro získání dat z pole. Výhodou pole typu RAID 0 je jeho rychlost. Jelikož zapisování probíhá rovnoměrně na všechny disky, dochází k využití rychlosti každého disku (Můčka, 2021). Největší nárůst rychlosti nastává při přidání druhého disku, v porovnání s rychlostí jednotlivého disku mimo pole RAID. S každým dalším přidaným růstem je zrychlení menší, ale stále znatelné.

RAID 1

Diskové pole typu RAID 1 neposkytuje žádné výhody v souvislosti se zvětšováním dostupného prostoru, nebo v souvislosti s rychlostí zápisu. Probíhá zde zrcadlení dat, kdy data jsou zaznamenávána rovnoměrně na dva disky zároveň. V praxi to poskytuje velmi efektivní ochranu zapisovaných dat, jelikož jsou k dispozici vždy dvě kopie, a tak může jeden ze dvou disků kompletně přestat fungovat a celá data budou zachována. V závislosti

na konkrétní implementaci v řadiči může pole RAID 1 poskytovat lehce vyšší rychlost čtení oproti použití samostatného disku, rychlost zápisu je buď stejná, nebo horší (Můčka, 2021). Hlavní nevýhodou tohoto typu diskového pole je, že výsledná dostupná kapacita je rovna velikosti menšího z disků.

RAID 5

Diskové pole typu RAID 5 využívá paritu, kdy je vypočítána parita ze zapisovaných dat a je spolu s daty zapisována na disk. Tato parita se využívá v případě poškození části dat k dopočítání těchto ztracených částí. V případě RAID 5 je parita rozdělena rovnoměrně mezi všechny zapojené disky a svou velikostí je rovna velikosti jednoho disku. Díky paritě dokáže pole typu RAID 5 zachovat data i po ztrátě jednoho celého disku. Tento ztracený disk je nutné nahradit novým prázdným diskem a spustit obnovu pole. Řadič poté z dostupných paritních dat vypočítá data, která byla na ztraceném disku a zapíše je na nový disk. Podle velikosti disků se odvíjí délka tohoto procesu, který může trvat v extrémních případech i několik dní. K vytvoření pole typu RAID 5 jsou potřeba minimálně tři disky.

RAID 6

RAID 6 se oproti RAID 5 liší v počtu paritních bloků uložených na každém disku. Zatímco RAID 5 ukládá na každý disk jeden paritní blok, RAID 6 na každý disk dává paritní bloky dva. Díky vyššímu počtu paritních dat dokáže toto pole rekonstruovat data i při ztrátě dvou disků. Rezervovaná kapacita pro paritní data v poli RAID 6 je rovna velikosti dvou disků. Minimální počet disků pro toto pole jsou 4, kdy kapacita dvou disků je dostupná pro ukládání dat, a kapacita dvou disků je využita pro paritní data.

3.1.3 Složené typy RAID polí

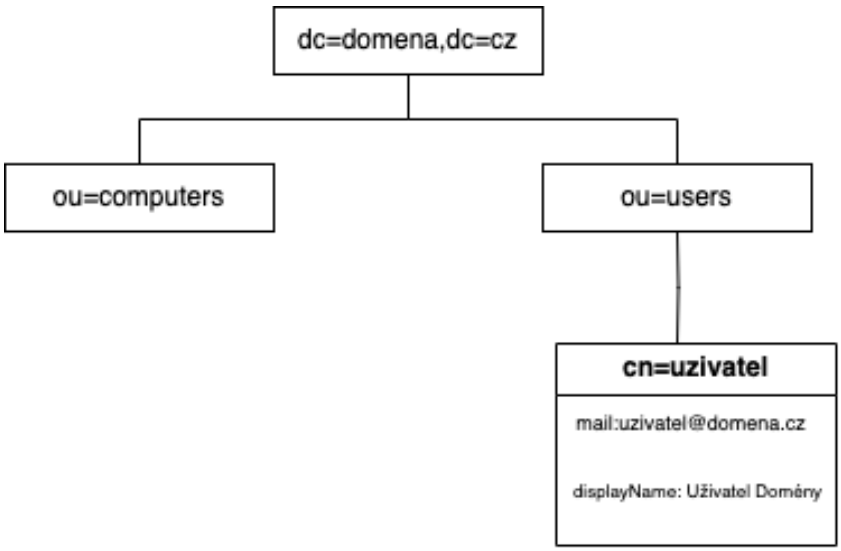
V praxi jsou často žádoucí kombinace vlastností více druhů polí. V takových případech se využívá složených RAID polí, kdy jsou disky spojeny po menších částech do polí jednoho druhu a tato dílčí pole jsou poté spojena do velkého diskového pole jiného druhu. Mezi často používané typy složených polí patří například RAID 01, ve kterém jsou disky spojeny po dvou do RAID 0 a tyto jsou pak spojeny do RAID 1, díky čemuž poskytuje výsledné pole rychlostní výhody pole RAID 0 a zároveň částečnou ochranu dat díky RAID 1 (Můčka, 2021). Další často používané typy složených polí jsou například RAID 50, RAID 60 a RAID 100.

3.2 LDAP

LDAP, zkratka pro anglické Lightweight Directory Access Protocol, česky Lehký Protokol pro přístup k adresáři, je protokol pro přístup a správu dat uložených na adresářovém serveru. Vychází ze specifikace X.500, která byla vyvinuta v rámci ISO/OSI, ale byla později označena za zbytečně komplikovanou a složitou. Od tohoto faktu se odvozuje slovo „Lightweight“ v názvu LDAP. LDAP využívá komunikaci prostřednictvím TCP/IP a je založen na architektuře klient/server, kdy na serveru je uložena databáze s informacemi o síti, také nazývána jako adresář, a klient k této databázi přistupuje přes počítačovou síť

3.2.1 Informační model

V LDAP jsou všechna data ukládána na adresářovém serveru do adresáře v podobě objektů. Adresář má logickou strukturu, která se nazývá adresářový strom (anglicky Directory Information Tree). Jednotlivé položky ve stromu se dále dělí na uzly a listy. List je samostatný koncový objekt a uzel definuje větvení adresářového stromu. Položky v databázi tedy nejsou ukládány do jedné roviny, ale jsou rozčleněny od hierarchicky uspořádaných skupin. Každý adresářový strom má definované schéma, které definuje, jaké objekty lze v adresáři uchovávat, jaké existují třídy objektů a jaké všechny atributy mohou objekty mít. Kořenovým bodem adresářového stromu je rootDSE, který obsahuje základní informace o adresáři (Bouška, 2007).



Obrázek 1: Logická struktura LDAP adresáře (Zapletal, 2000)

Každý objekt je identifikován unikátním jménem, má určenou svou třídu a obsahuje několik atributů. Třída objektu určuje, jaké atributy může daný objekt obsahovat. Pokud si například nadefinujeme třídu osoba, můžeme jí přiřadit atributy jméno, příjmení, adresa a telefonní číslo. Jeden objekt může být součástí několika tříd a v takovém případě může obsahovat dohromady atributy ze všech tříd, do kterých je zařazen. Atributy jsou identifikovány unikátním jménem v rámci objektu. Pokud je objekt zařazen do více tříd, které obsahují některé totožné atributy, budou tyto atributy u objektu sloučeny do jednoho. Atributy mají v rámci schéma definovaný typ hodnoty, který do nich lze uložit, a také zda je nutné je vyplnit nebo jsou volitelné.

3.2.2 **Jmenný model**

Jmenný model protokolu LDAP určuje, jakým způsobem může klient přistupovat k jednotlivým objektům v adresáři a k tomu se využívá rozlišovací jméno (anglicky Distinguished Name) (Sitera, 2000). To se skládá z vlastního jména objektu a jmen objektů, přes které vede cesta od kořene stromu až k danému listu.

Tyto názvy jsou zapsány ve formátu XX=YYYY, kde XX je zkratka určující název atributu a YYYY je hodnota obsažená v atributu. Pro příklad rozlišovací jméno uživatele User, který je členem organizační jednoty OrgJednotka v doméně domena.cz by vypadalo následovně: DN = cn=User, ou=OrgJednotka, dc=domena, dc=cz. Na tomto příkladu je možné vidět několik zkratek. Cn je zkratka pro anglické common name a jedná se o unikátní jméno objektu v Adresáři. Ou zde označuje organizační jednotku, což je kontejnerový objekt, který v adresáři slouží k organizaci objektů. Dc je zkratka pro domain component, neboli doménová část, a obsahuje název domény rozdělený v místě teček. Pokud se v adresáři úkony provádí v rámci jednoho konkrétního kontejneru, je možné využít relativní rozlišovací jméno (Relative Distinguished Name), které obsahuje pouze common name. V situaci uvedené v dřívějším příkladu by tedy relativní rozlišovací jméno vypadalo takto RDN = cn=User.

Mimo rozlišovací jména má každý objekt v adresáři přiřazené ještě unikátní 128bitové identifikační číslo GUID, které se nemění, pří editaci atributů nebo přesouvání v rámci struktury adresáře a lze podle něj k objektu přistupovat (Sitera, 2000).

3.2.3 **Funkční model**

Funkční model určuje fungování operací, které může uživatel s Adresářem provádět. Protokol LDAP obsahuje celkem 9 operací, které jsou rozřazeny do tří kategorií. Tyto kategorie jsou autentizace, dotazování a aktualizace.

Do kategorie autentizačních operací patří operace související s ovládáním komunikace se serverem, jedná se o operace bind, unbind a abandon (Sitera, 2000). Operace bind slouží k navázání spojení klienta se serverem. Operace nejdříve zkontaktuje server a vyjedná s ním specifikace autentizace a poté serveru odešle přihlašovací údaje klienta, podle kterých proběhne samotná autentizace. Operace unbind jednoduše ukončí komunikaci mezi klientem a serverem. Operace abandon slouží ke zrušení zpracování předchozího dotazu. Při uplatnění této operace přestane server předchozí dotaz zpracovávat a nevrátí klientovi žádné jeho výsledky.

Kategorie dotazovacích operací obsahuje pouze dvě operace – search a compare (Bouška, 2007). Pro čtení dat z adresáře slouží operace search. Pro tuto operaci je nutné určit několik parametrů, podle kterých čtení dat z adresáře proběhne. V parametru filtr se určuje, jaké parametry, se kterou hodnotou má server u objektů vyhledávat. Dalším důležitým parametrem je báze, která reprezentuje nejvyšší bod stromu, který bude prohledáván. Pokud chce uživatel pracovat na celém stromu, jako báze se určí jeho kořen a pokud chce uživatel prohledávat pouze určitou část stromu, jako báze se určí nejvyšší společný bod všech žádoucích objektů. V takovém případě se většinou jedná o organizační jednotku. Dalším parametrem je rozsah, který určuje, jestli se bude prohledávat pouze definovaný bázový objekt, nebo i části jeho podstromu či celý podstrom. V rámci operace search je možné omezit, které parametry od nalezených objektů server vrátí klientovi. Operaci search lze pomocí parametrů omezit na určitý počet nalezených položek, nebo na určitý časový úsek. Operace compare provede porovnání hodnoty atributu konkrétního objektu v Adresáři s hodnotou určenou klientem. Poté klientovi vrací logickou hodnotu true, nebo false.

Třetí kategorie, kategorie aktualizačních operací obsahuje čtyři operace, kterými jsou add, modify, modify RDN a delete (Bouška, 2007). Operace add slouží k vytvoření nového objektu v adresáři. V rámci této operace je nutné definovat unikátní název objektu, jeho umístění ve stromové struktuře a hodnoty všech povinných atributů. Naopak operace delete smaže z adresáře existující položku. Tato operace je omezena pouze na listy stromu, tudíž odmítne smazat objekt, pokud mu ve stromové struktuře jsou nějaké jiné objekty přímo podřízeny. Operace modify dokáže editovat hodnoty atributů, vytvářet u objektů nové

atributy a také existující atributy mazat. Poslední operace modifyRDN slouží k upravování rozlišovacího jména objektu. V praxi se tedy používá k přesouvání objektů v rámci stromové struktury adresáře

3.2.4 **Bezpečnostní model**

Bezpečnostní model protokolu LDAP se dělí na 3 základní kategorie: autentizace, zabezpečení komunikace a autorizace. Autentizace slouží k ověření identity uživatele, nebo jiného objektu v rámci adresáře. K autentizaci v LDAP se používají SASL (Simple Authentication and Security Layer) mechanismy. SASL mechanismy nejsou v protokolu pevně definovány a existuje jich celá řada druhů. Informace o tom, které SASL mechanismy konkrétní adresářový server podporuje je uložena v atributu supportedSASLMechanisms v kořenovém záznamu adresáře.

Mezi často používané SASL mechanismy patří PLAIN, což je autentizace pomocí jména a hesla v nešifrovaném čistém textu. Pro ověření pomocí jména a hesla v šifrované podobě se používá mechanismus DIGEST-MD5, který neodesílá na server celé heslo, ale pouze jeho MD5 hash. Kontroluje také integritu a důvěrnost spojení mezi klientem a serverem. Mechanismus ANONYMOUS nepoužívá žádné autentizační informace a až na okrajové případy je kvůli bezpečnosti na adresářových serverech deaktivován. (Sitera, 2000)

3.3 **DNS**

DNS je systém, který slouží k překládání doménových jmen, na příslušné IP adresy a IP adres na doménová jména. V případě že klient potřebuje komunikovat se serverem a jeho jméno je uvedeno v DNS formátu XXX.YYYY.ZZ, klient odešle na lokální DNS server, který byl předem určen správcem sítě při konfiguraci připojení, požadavek o překlad DNS názvu na jemu přidělenou IP adresu. Tento DNS server potom vyhledává odpovídající IP adresu pro zadanou doménu. Pokud nemá požadovanou odpověď v cache, může přesměrovat dotaz na další vyšší úroveň DNS serverů, dokud nenajde odpovídající záznam.

Celý systém DNS je hierarchicky organizován do stromové struktury, která se skládá ze zón, domén a DNS serverů. Nejvyšší úroveň této hierarchie představuje kořenové DNS servery, které jsou zodpovědné za adresování dotazů na nejvyšší úroveň doménových koncovek (TLD), jako jsou .com, .org, .net atd. Pod TLD jsou další úrovně, jako jsou druhé úrovně doménových jmen (SLD), jako například domena.cz.

DNS funguje na základě distribuované databáze, která obsahuje záznamy přiřazení názvů domén k IP adresám. Tyto záznamy jsou ukládány do tzv. DNS zón, které jsou spravovány jednotlivými autoritativními DNS servery. Existují různé typy DNS záznamů, jako A (adresový) záznam, který mapuje název domény na IPv4 adresu, nebo AAAA záznam, který mapuje doménu na IPv6 adresu. Dalšími běžnými typy jsou MX záznamy pro určení poštovních serverů, CNAME záznamy pro aliasy, nebo TXT záznamy pro různé druhy textových informací. (CZ.NIC,2017)

3.4 Active Directory

Active Directory je adresářová služba od společnosti Microsoft, což je sada aplikací a služeb, které uchovávají informace o objektech v počítačové síti a poskytuje řadu dalších služeb v síti. Mezi tyto služby patří například autorizace a autentizace uživatelů a počítačů v doméně, správa přístupů k síťovým prostředkům, aplikování doménových politik, instalace a aktualizace softwaru, nebo například vydávání, distribuce a správa certifikátů. Ke zprostředkovávání těchto služeb používá Active Directory protokoly LDAP a Kerberos a služby DNS serveru.

3.4.1 Historie Active Directory

Active Directory není první doménový produkt od společnosti Microsoft. Pro potřeby systému Windows NT, poprvé vydaného v roce 1993, vyvinula společnost Microsoft službu Microsoft Domain. Objekty v Microsoft Domain nebyly uloženy hierarchicky, ale v nehierarchické databázi, označované jako SAM (Security Account Manager). Neexistovaly tedy OU a objekty nebylo možno nijak logicky rozřadit. Primární funkce Microsoft Domain bylo přihlašování uživatelů a poskytování přístupů k síťovým prostředkům na základě přiřazení uživatele ke skupině s oprávněními

Hlavní nevýhodou této služby byla absence struktury v adresáři, která u velkých sítí způsobovala komplikace při správě uživatelů a jejich přístupů. Zároveň nešly domény seskupovat do lesů, což znamenalo že rozsáhlé sítě, které potřebovaly více doménových řadičů, měly problémy se správou, kdy každá změna nemohla být provedena centrálně, ale musela být manuálně uskutečněna na každém doménovém řadiči. Microsoft Domain také závisela na tehdy již zastaralých technologiích, jako byly NTLM (v AD nahrazena protokolem Kerberos), NetBIOS (v AD nahrazen DNS) a NetBEUI (v AD nahrazen protokolem TCP/IP) (Thurrott, 2000).

Kvůli těmto nedostatkům se Microsoft již v roce 1993, v rámci plánování projektu Cairo, rozhodl, že vyvine novou adresářovou službu, podle specifikace x.500 (Microsoft Corporation, 1993). Tuto novou službu pod názvem Active Directory Microsoft poprvé představil na konferenci PDC 1996. V září 1997 byla pro veřejnost vydána první beta verze Active Directory pro Windows NT 4.0, druhá beta verze, která už byla prakticky kompletní, byla zveřejněna v říjnu 1999 a v únoru roku 2000 byla vydána verze Windows 2000 Profesional pro počítače, spolu s verzí Windows Server 2000 pro servery (Thurrot ,1999). Tyto verze již měly AD a nástroje pro správu AD integrované v sobě. Pro starší verze Windows - 95, 98 a NT 4.0 byly vydány volitelné aktualizace, které přidávaly částečnou podporu pro zařazení do AD. Vývoj Active Directory aktivně pokračuje až dodnes, kdy každá nová verze Windows Server přináší nové funkce a vylepšení.

Windows Server 2003 přidal možnost pro různé skupiny uživatelů aplikovat jiné požadavky na hesla a Application Mode, který umožňuje provozovat AD v omezeném režimu, ve kterém se AD chová jako jednoduchý LDAP server, ale nadále umožňuje správu pomocí pokročilých nástrojů pro správu Active Directory (Svidergol, 2017). Windows Server 2008 nově zahrnoval služby federace Active Directory, které umožňují mezi organizační přihlašování ke službám a koš pro Active Directory, který umožňuje obnovit omylem smazané objekty (Svidergol, 2017). Windows Server 2008 R2 představil PowerShellový modul pro Active Directory, který umožňuje správu pomocí příkazového řádku PowerShell a nový nástroj pro správu AD s názvem Administrative, verze Windows Server 2012 R2 představila metodu připojení do domény Workplace Join, která umožňuje zařízení přistupovat k prostředkům v doméně, aniž by se stalo plnohodnotným členem domény a Windows Server 2016 přinesl funkcionalitu Azure AD join, která slouží k integraci Active Directory se službou Microsoft Azure Active Directory (později přejmenovanou na Azure Entra ID) (Svidergol, 2017).

3.4.2 **Struktura domény Active Directory**

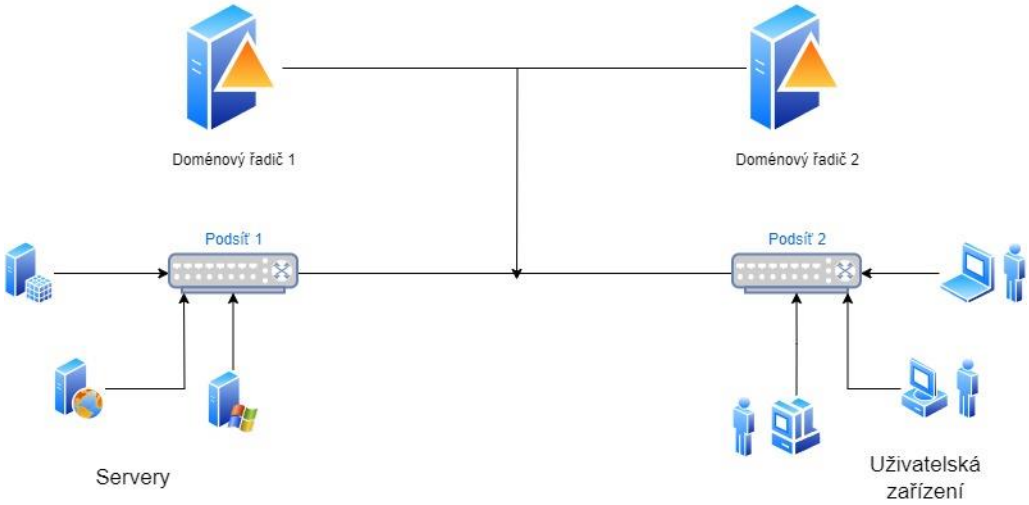
Doména označuje logickou skupinu počítačů, které mají společnou AD databázi. Všechny objekty (uživatelé, počítače, distribuční a zabezpečovací skupiny…), které jsou ve správě Active Directory, se označují jako členové domény. Hlavní server, na kterém jsou uloženy všechny údaje v adresáři, který zprostředkovává všechny služby AD a který zároveň funguje jako hlavní DNS server, se označuje názvem doménový řadič. Těchto doménových řadičů může v doméně být více, pro případ, kdy by jeden z nich přestal fungovat, nebo

z důvodu rozložení zátěže mezi více serverů. Z hlediska struktury jsou tyto doménové řadiče rovnocenné. Změny provedené na kterémkoliv z nich jsou synchronizovány pomocí multi-master peer-to-peer replikace, kdy při změnách vyšle Doménový Řadič zprávu, že byly provedeny změny a ostatní doménové řadiče si přímo od něj tyto změny stáhnou a provedou na svých kopiích databáze.

Podle specifikací (Microsoft Corporation, 2009) logické uložení objektů v adresáři funguje na stejném principu jako u LDAP, tedy na principu stromového uspořádání . Odtud se odvozují pojmy strom a les. Strom označuje hierarchickou strukturu jedné, nebo více domén, které sdílí jmenný prostor (Bouška, 2008). Jména hierarchicky podřízených domén se tvoří ze zvoleného jména podřízené domény, tečky a jména nadřízené domény. Les označuje hierarchickou strukturu více nezávislých domén, které sdílí stejný kořen a konfiguraci. Tyto domény nesdílí jmenný prostor a fungují nezávisle, ale mohou mezi sebou díky lesu komunikovat.

Fyzicky jsou data uložena na disku doménových řadičů v souboru NTDS.DIT. Tento databázový soubor používá technologii Extensible Storage Engine, což je databázový systém specificky pro využívání součástmi operačního systému Windows (kromě Active Directory jej používá například Microsoft Exchange pro ukládání emailových schránek, nebo vyhledávání ve Windows pro indexování souborů na disku.) K této databázi jako takové ale nemá správce přímý přístup a veškerá správa probíhá přes nástroje pro správu domény.

Fyzická struktura domény se skládá z doménových řadičů a podsítí. Tyto podsítě mají daný rozsah IP adres a jsou do nich připojena zařízení, které jsou součástí Active Directory. Active Directory tyto podsítě mapuje a mapy poté využívá ke směřování klientů ke komunikaci s Doménovým Řadičem, který je v rámci sítě nejblíže.



Obrázek 2: Fyzická struktura Active Directory (Microsoft Corporation, 2009)

3.4.3 Objekty v Active Directory

Všechny zdroje dostupné v doméně Active Directory jsou v adresáři uloženy jako objekty (Bouška, 2014). Každý objekt má při založení přiřazený jedinečný identifikátor GUID (Globally Unique Identifier). Tento identifikátor se po celou dobu existence objektu nemění a není závislý na jeho umístění v rámci stromu adresáře. Podobně jako u protokolu LDAP jsou objekty rozřazeny do dvou kategorií: kontejnery a listy stromu. Mezi kontejnery se řadí objekty typu organizační jednotka a skupina. Vyznačují se tím, že obsahují další objekty. Mezi listy stromu se řadí například uživatelé, počítače a sdílené složky. Tyto listy nemohou obsahovat další objekty a jsou tedy koncovými body stromu adresáře. V doméně se navíc některé objekty označují jako Security Principal, což jsou entity, které se mohou autentifikovat k přístupu k prostředkům v rámci AD. V praxi se mezi ně řadí uživatelé, počítače a bezpečnostní a distribuční skupiny. Oproti ostatním objektům se těmto Security Principal přiděluje SID (Security Identifier), který se používá při přidělování a správě oprávnění k doménovým prostředkům (Bouška, 2014).

Uživatelské účty by správně měly reprezentovat v adresáři konkrétního člověka, který přistupuje k síťovým prostředkům v doméně, i když se v praxi často setkáváme se situacemi, kdy je uživatelský účet sdílený mezi více uživateli. V adresáři lze k uživateli uložit například jeho jméno, kontakty, kancelář, nebo přímé nadřízené a podřízené. Pro identifikaci uživatele v doméně se používá atribut commonName, z něhož se poté pro potřeby autentifikace skládá sAMAccountName ve formátu domena\commonName a UserPrincipalName ve formátu commonName@domena. K uživatelskému účtu se také dá přistupovat pomocí LDAP

konstruktu Distinguished Name v podobě CN=commonName OU=organizačníJednotka DC=domena.

Počítače uložené v adresáři označují důvěryhodné pracovní stanice a servery. Objekt pro konkrétní počítač se vytvoří automaticky v momentě zařazení tohoto počítače do domény. Mezi detaily objektu typu počítač patří například název počítače, DNS název počítače ve formátu nazevPocitace.domena, verze operačního systému, nebo doba posledního přihlášení k doméně.

Zabezpečovací a distribuční skupiny mohou obsahovat uživatele, počítače, nebo další skupiny z domény. Smyslem zabezpečovacích skupin je zjednodušení správy oprávnění k síťovým prostředkům v doméně a aplikování skupinových politiky, kdy oprávnění, respektive skupinová politika, jsou přiděleny skupině a z ní je dědí všichni její členové. Distribuční skupiny se zpravidla používají k hromadné distribuci zpráv mezi vícero příjemců. Například v případě emailového systému Microsoft Exchange má distribuční skupina přidělenou vlastní emailovou adresu, a zprávy odeslané na tuto adresu jsou rozeslány mezi všechny členy skupiny. Členství v distribuční skupině neposkytuje členům žádná další oprávnění v rámci domény.

Organizační jednotky slouží ve stromu adresáře jako uzly, jedná se tedy o kontejnery obsahující další objekty. Jejich primární využití je určování vlastní struktury stromu adresáře. Dalším z významných využití organizačních jednotek je určování rozsahu aplikování skupinových politik. Skupinovou politiku lze zaměřit na konkrétní organizační jednotku a působení politiky bude omezeno pouze na její členy. V rámci Active Directory, na rozdíl od jiných adresářových služeb, není možné používat organizační jednotky pro přidělování oprávnění k doménovým prostředkům.

3.5 Samba

Samba je softwarový balík, který má za cíl umožnit komunikaci pomocí protokolu SMB v Unixových operačních systémech. U moderních operačních systému, které zároveň nejsou vytvořeny společností Microsoft, se jedná o defacto standard pro komunikaci přes SMB. Z hlediska systému se zpravidla jedná o dvě systémové služby. Smbd je služba, která se stará o samotné přistupování a sdílení složek a tiskáren a služba nmbd překládá názvy počítačů podle NetBIOS na jejich IP adresu v síti. V případě že se Samba používá ve spojení s doménou Active Directory jako klient nebo jako doménový řadič, využívá se služba winbindd, která celou tuto funkcionalitu zprostředkovává. Uživatelům Samba poskytuje

mnoho nových příkazů do příkazové řádky, které umožňují obsluhu sdílených síťových prostředků. Například příkaz smbclient umožňuje navázat spojení se serverem a provádět operace se soubory a příkaz smbget slouží ke stahování souborů ze vzdáleného serveru pomocí SMB. Sambu lze využít také jako knihovnu pro programování, což využívají například různí Linuxoví správci souborů, aby umožnili procházení sdílených složek na síti podobně, jako to funguje v průzkumníku v operačním systému Windows.

3.5.1 **SMB**

Server message block (SMB) je protokol pro sdílení souborů, tiskáren a dalších komunikačních zařízení po síti. Byl vyvinut firmou IBM v roce 1983 pro síťové složky pro DOS a později rozšířen a upraven pro použití v operačním systému IBM OS/2. V roce 1993 jej Microsoft převzal od IBM jako svůj standard pro síťové sdílení a implementoval ho do operačního systému Windows NT 3.1. V roce 1996 zveřejnil Microsoft návrh pro adoptování lehce upravené verze protokolu SMB pod názvem Common Internet File System (CIFS), jako všeobecného otevřeného standardu pro sdílení souborů po síti. Tento návrh nakonec nebyl přijat a Microsoft nadále pokračoval ve vývoji SMB, ale pokračoval také ve zveřejňování specifikací nově přidaných a upravených funkcí, což umožnuje ostatním výrobcům implementovat tyto funkce a vyrábět se SMB plně kompatibilní zařízení (Microsoft Corporation, 2012).

Při vývoji SMB 2.0 se Microsoft soustředil na zeštíhlení kódu, což vedlo k vynechání některých málo využívaných funkcí. Pokud klient nebo server potřebovali tyto funkce využít, komunikace se automaticky navrátila na protokol SMB 1.0. Příkladem takovéto funkce je podpora komunikace pomocí kódování Unicode, která byla na původní protokol SMB přidělávána později, a tak byly s ní související příkazy komplikované. Jelikož již v době vývoje SMB 2.0 drtivá většina komunikace přes SMB probíhala právě s kódováním Unicode, bylo rozhodnuto, že u SMB 2.0 bude veškerá komunikace automaticky probíhat s kódováním Unicode a ostatní kódové sady nebudou podporovány. Verze SMB 2.0 přidala podporu symbolických linků, vylepšila podporu podepisování přenášených datových bloků a zlepšila rychlost přenosu velkých souborů, díky podpoře větší velikosti datových bloků. Další vylepšení v SMB 2.0 spočívaly ve zjednodušování. Verze SMB 1.0 obsahovala okolo stovky příkazů a podpříkazů, oproti tomu SMB 2.0 snížila tento počet na devatenáct. Zároveň přibyla příležitost sloučit více požadavků do jedné zprávy, což snižuje vytížení sítě při komunikaci.

Verze SMB 3.0 přinesla protokol SMB direct, který umožňuje síťovému adaptéru zapisovat přímo do paměti počítače bez účasti operačního systému, což umožňuje vyšší přenosové rychlosti. Další funkcí pro zvýšení přenosové rychlostí je SMB Multichannel, který umožňuje klientovi navázat se serverem více paralelních připojení. To je výhodné při přenosu většího množství souborů, jelikož lze přenášet více souborů navíc a využít tím naplno schopnosti sítě. SMB transparent failover slouží k zrcadlení jedné sdílené složky na více serverů pro případ výpadku nebo údržby. V případě že se hlavní server stane nedostupným, komunikace se automaticky přesměruje na ostatní servery s danou sdílenou složkou. Klient v takovém případě ani nezaznamená, že k nějaké změně došlo. Po obnovení přístupnosti hlavního serveru se změny provedené na vedlejších serverech nejdříve přenesou na hlavní server, a pak se komunikace přesune zpět na hlavní server. Od roku 2017 je protokol SMB 1.0 považován za nebezpečný a je jej doporučeno na serverech a klientských zařízeních deaktivovat, pokud jeho přítomnost není bezpodmínečně nutná pro fungování starého vybavení, nebo softwaru.

Komunikace v protokolu SMB probíhá přes tzv. zprávy (Hertel, 2003). Ty se skládají ze tří hlavních částí – hlavičky, parametrů a dat. Hlavička vždy začíná identifikátorem protokolu 0xffSMB. Následuje bajt příkazu, který určuje typ SMB komunikace a po něm 32bitů dlouhý prostor pro stavovou proměnnou. Dále jsou v hlavičce dvě pole pro vlaječky, ve kterých se přenáší informace o využitích rozšiřujících funkcích protokolu. Další sekce hlavičky se označuje jako extra a obsahuje dvě pole. První z nich je PidHigh, ve kterém se ukládá druhá polovina ID procesu SMB pro systémy, které využívají 32bitové procesové ID. Druhé pole se využívá pro kryptografický podpis komunikace. Na konci hlavičky se nachází TID, které identifikuje, se kterou konkrétní sdílenou složkou na serveru klient komunikuje, PID, ve kterém se ukládá první polovina ID procesu, který požadavek na server odesílá, UID, což je ID uživatele autentifikovaného k serveru a MID, které se používá ke spárování odpovědi s požadavkem v případě, že server má od klienta více nevyřízených požadavků. Parametry v komunikaci SMB se liší u každého typu příkazu, všeobecně se o nich ale dá říct, že se jedná o parametry funkce, která je v rámci SMB komunikace vyvolávána. Na konci zprávy v SMB je blok s daty, který obsahuje samotná data, ohledně kterých komunikace probíhá. V případě čtecích operací tedy bude tento blok obsahovat data ze serveru, která si klient vyžádal a v případě zapisovacích operací se zde budou nacházet data, která chce klient na server uložit.

3.5.2 **Historie a vývoj Samby**

S vývojem bezejmenného projektu, který až později dostal název Samba, začal Andrew Tridgell v roce 1992. Jelikož SMB byl původně uzavřený protokol, jehož způsob fungování nebyl veřejnosti přístupný, analyzoval Tridgell odchycené komunikační pakety a postupně tak odhalil princip fungování a mohl jej implementovat ve svém softwaru. První verze tohoto softwaru měla omezenou funkčnost a její implementace protokolu SMB byla primitivní, přesto se rychle rozšířila mezi tehdejší počítačové nadšence. V průběhu roku 1993 se Tridgellovi dostaly do rukou specifikace protokolu SMB, podle kterých přepsal značnou část kódu, což vedlo k výraznému zlepšení kompatibility s ostatními systémy používajícími protokol SMB (Tridgell, 1994). Tuto přepracovanou verzi vydal v prosinci roku 1993 pod názvem smbserver. Práce na smbserveru pokračovaly svižným tempem, což znamenalo postupné vylepšování stability a rychlosti a zároveň rozšiřování funkcionality. V dubnu roku 1994 byli vývojáři kontaktováni společností Syntax Corp, jelikož Syntax Corp byla držitelem ochranné známky na název smbserver, a tak museli vývojáři vymyslet jiný název. Chtěli zachovat odkaz na SMB protokol v názvu, a tak vyhledali v unixovém systémovém slovníku všechna slova, která obsahují po sobě jdoucí písmena S, M a B. Ze slov, která splňovala tento požadavek nakonec vybrali slovo samba, což je název latinskoamerického tance. (Tridgell 2002)

Na počátku se vývojáři projektu Samba soustředili na dosažení funkčnosti Samby na stejné úrovni v oblasti sdílených složek a tiskáren s ostatními řešeními na protokolu SMB, primárně tedy s Windows NT Server, Microsoft Lan Manager a IBM OS/2 Lan Server. Od verze Samba 2.2 byly přidány experimentální funkce, které umožňovaly Sambě fungovat jako klient nebo primární doménový řadič v doméně Microsoft Domain (Tranquil IT, 2023). Při vývoji verze Samba 3.0 se vývojáři rozhodli postupně přidat funkcionalitu pro tehdy novou doménovou službu společnosti Microsoft – Active Directory. Samba 3.0, která vyšla v září roku 2003, přidala nově podporu připojení do domény Active Directory jako klient a z toho vyplývající autentifikace doménovými uživatelskými účty. Zatím stále chyběla možnost využívat Sambu jako doménový řadič pro Active Directory. Ve verzi Samba 3.6 byla implementována plná podpora protokolu SMB 2

V roce 2005 byl spuštěn v rámci vývojového týmu nový projekt Samba4. Od dob původního zpětného inženýrství SMB Andrewem Tridgellem se situace ohledně uzavřenosti tohoto protokolu změnila a společnost Microsoft zveřejnila své oficiální specifikace pro SMB. Vývojáři se tedy rozhodli celou Sambu kompletně přepsat podle těchto specifikací.

Zároveň s přepisováním komponent pro sdílení souborů a tiskáren, probíhala implementace funkcionality doménového řadiče, také podle specifikací Microsoftu. V roce 2012 si vývojáři uvědomili, že specifikace protokolu SMB od Microsoftu jsou stále nedostatečné, a tak došlo ke sloučení nově implementovaných funkcí s původním kódem se Samby 3. Tato vývojová cesta se ukázala jako úspěšná a v prosinci roku 2012 byla vydána verze Samba 4.0, která nově podporovala možnost Sambu používat jako plně funkční doménový řadič Active Directory. Od vydání verze 4.0 až dodnes přináší každá další vydaná verze nové funkce. Ve verzi 4.1 přibyla plná podpora protokolu SMB 3.0, verze 4.2 přinesla podporu komprese dat při použití souborového systému BTRFS a mapování doménových uživatelů a skupin na lokální unixové uživatele a skupiny pomocí služby winbindd. Další důležitou součástí fungování klienta v rámci domény Active Directory je autentifikace pomocí protokolu Kerberos, která do Samby přibyla s vydáním verze 4.7 (Tranquil IT, 2023).

4 Vlastní práce

4.1 Prostředí instalace

Obvodní soud pro Prahu 1 se nachází v historické budově v centru Prahy, na rohu ulic Celetná a na Ovocném Trhu. Lokální síť má hvězdicovou topologii, kde se ve středu hvězdice nachází serverovna v prvním patře. Zde jsou nainstalovány dva doménové řadiče Active Directory s operačním systémem Microsoft Windows Server 2016, které zároveň fungují jako DNS servery a DHCP servery. DNS název domény je a1.sou-pha.justice.cz a jeho krátká forma je SOUA1. Pro potřeby ukládání zvukových záznamů ze soudních jednání se zde také nachází rychlé diskové pole s rychlými SAS disky. Kapacita tohoto diskového pole přestává stačit, a tak bylo rozhodnuto, že bude jeden z přítomných nevyužitých pomalejších serverů využit pro dlouhodobější ukládání záznamů.

Pro potřeby této práce byl, převážně kvůli velkému úložišti, zvolen server Dell PowerEdge 2950 s procesorem Intel Xeon E5335, 10 GB DDR2 ECC RAM a diskovým polem SATA s kapacitou 8TB. Ačkoliv se jedná o starší stroj z roku 2007, disky byly v nedávné době vyměněny za nové a specifikace hardwaru pro využití jako souborový server stačí. Server sám o sobě obsahuje licenci pro Windows Server 2003, který je pro použití v moderním prostředí nevhodný, hlavně kvůli konci podpory od společnosti Microsoft, což znamená že jakékoli bezpečnostní zranitelnosti zůstávají neopravené a server je snadno napadnutelný. Nákup licence pro moderní verzi Windows Server by svou cenovkou nejspíše překonal cenové ohodnocení samotného serveru, a i když minimální požadavky pro instalaci by tento server splňoval, využívání by bylo nejspíše pomalé, protože velkou část výkonu by si operační systém zabral pro svoje vnitřní procesy a na obsluhu uživatelů, kteří by chtěli k souborům na fileserveru přistupovat, by zbylý výkon nemusel stačit. Proto bylo rozhodnuto, že na server bude nainstalován operační systém Linux, který je zdarma a má nižší základní hardwarové nároky. Na operační systém Linux bude poté nainstalován softwarový balík Samba, který umožňuje sdílení složek pomocí protokolu SMB a zařazení serveru do domény Active Directory, což bude umožňovat plynulou spolupráci nově nainstalovaného souborového serveru s existující počítačovou infrastrukturou na soudu.

4.2 Požadavky na souborový server

Server bude využit pro dlouhodobou archivaci starých zvukových záznamů ze soudních jednání, proto nebyly vzneseny žádné požadavky na rychlost přístupu. Hlavní

požadavky směřovaly na efektivní využití dostupného hardware a ochranu dat před selháním disku. Na základě dohody s vedením soudu byly na souborový server byly tedy zvoleny následující požadavky:

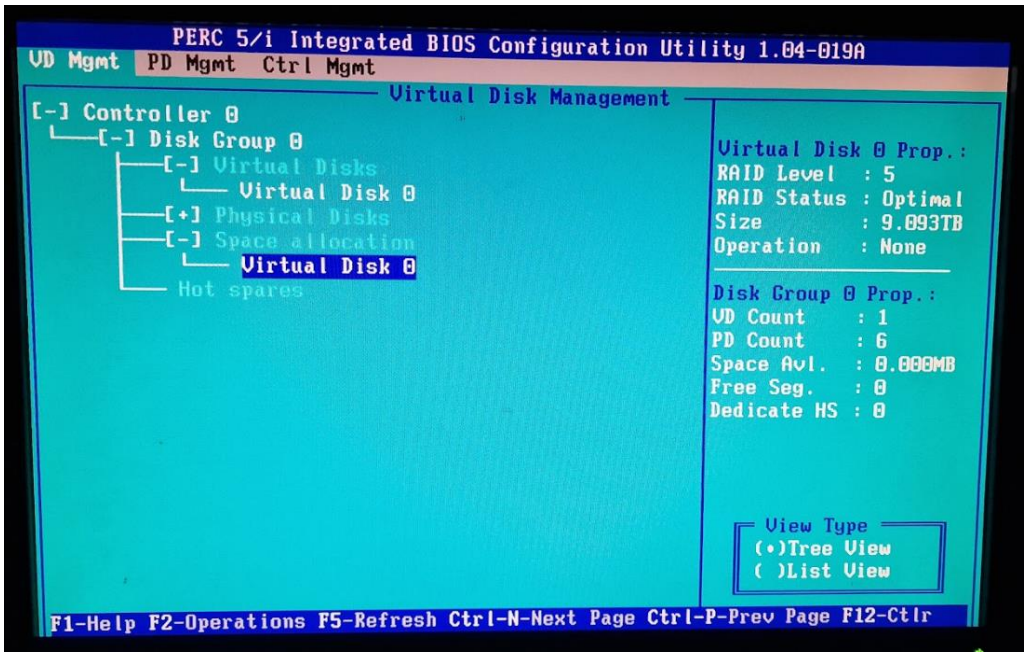
- Operační systém Linux s nejnovějšími bezpečnostními záplatami
- Využití všech disků serveru v diskovém poli RAID
- Odolnost pole RAID při selhání jednoho disku
- Zařazení serveru jako člena domény
- Využití protokolu SMB pro sdílené složky
- Řízení přístupů na základě doménových účtů a skupin

4.3 Vytváření pole RAID

Server využívaný pro tuto práci má všechny disky zapojeny do hardwarového RAID řadiče PERC 6/i SAS integrovaného na základní desce serveru. Pro konfiguraci RAID řadiče má server speciální rozhraní podobné konfiguračnímu rozhraní BIOS. Pro vstup do konfiguračního RAID prostředí je nutné zmáčknout klávesovou zkratku CTRL + R při zapínání serveru v momentě, kdy server projde POST testem a zinicializuje RAID řadič. Výzva ke stisknutí této klávesové zkratky se zobrazí na monitoru a na stisknutí server čeká 10 sekund. V případě že uživatel klávesovou zkratku nestiskne, pokračuje server se zaváděním operačního systému z disku.

Po zvážení všech možností bylo pro tento server zvoleno diskové pole typu RAID 5, jelikož poskytuje vysokou rychlost, díky prokládání dat na všechny disky, ale také jistou míru ochrany dat, kdy díky paritním datům dokáže bez ztráty dat ustát selhání jednoho z pevných disků. Při prvním naběhnutí do konfiguračního prostředí server oznámí, že není přítomna žádná existující konfigurace diskového pole a disky jsou označeny jako dostupné pro zařazení do nového diskového pole. V konfiguračním menu zvolíme možnost úplně nahoře, která reprezentuje RAID řadič, a v menu u ní vybereme možnost Create New VD neboli vytvořit nový virtuální disk. V nově zobrazeném okně zvolíme typ pole RAID 5 a v pravé části, kde je vypsán seznam všech harddisků zapojených do RAID řadiče, zaškrtneme postupně každý disk a potvrdíme tlačítkem ok. V seznamu se nově zobrazil v kategorii Virtual Disks námi nově vytvořený virtuální disk. Zvolíme jej a spustíme rychlou inicializaci. Nyní, když je pole vytvořeno a zinicializováno, můžeme tlačítkem escape odejít z RAID konfiguračního prostředí. Následně se na monitoru zobrazí výzva k restartování

serveru klávesovou zkratkou CTRL + ALT + DELETE. Po restartu je diskové pole RAID 5 dostupné pro operační systém v podobě jednoho velkého virtuálního disku.



Obrázek 3: Konfigurační prostředí RAID

4.4 Operační systém Linux

4.4.1 Výběr distribuce OS Linux

Operační systém Linux je dostupný v mnoha různých distribucích, což jsou kompletní systémová řešení, která obsahují Linuxové jádro a všechen ostatní software, který je potřeba k tomu, aby Linux byl plnohodnotným operačním systémem. Obsahují tedy vše od zaváděcího programu, přes správce softwarových balíčků, až po textové editory. Každá tato distribuce má svou specifickou sadu softwarových balíčků a výběr konkrétní distribuce se odvíjí od požadavků na vlastnosti tohoto softwaru. Jelikož od serveru se požaduje vysoká míra stability a spolehlivosti, je výběr hlavně diktován stabilitou a ověřenou funkčností balíčků v repozitářích. Dalšími kritérii je rozsah dostupných softwarových balíčků a nástrojů v repozitářích a komunitní dokumentace k těmto balíčkům. Na základě těchto kritérií je v rámci této práce zvolena distribuce Ubuntu Server, která vychází ze základní distribuce Debian, ale oproti ní poskytuje častější aktualizace softwarových balíčků a větší počet softwarových balíčků v repozitářích.

4.4.2 **Instalace OS Ubuntu Server**

Instalační obraz operačního systému Ubuntu Server je dostupný ke stažení z oficiálních webových stránek ubuntu.com vždy ve dvou variantách. První variantou je verze LTS, která vychází každý druhý rok v dubnu a vyznačuje se tím, že má zaručené bezpečnostní aktualizace na 5 let od vydání pro všechny balíčky v repozitáři. To umožňuje uživatelům zůstat po celou dobu podpory u stejných verzí programů, které dostávají pouze bezpečnostní aktualizace, ale jinak se nemění, čímž je zaručena jejich stabilita. Po uplynutí pěti let je možné přejít na další verzi LTS, zde už ale není zaručeno, že se při přechodu nějaký softwarový balíček významně nezmění, nebo nerozbije.

Druhá varianta nemá v názvu LTS, vychází každý půlrok a nezdržuje verze balíčků. Výhodou této varianty je možnost používat nové verze softwaru brzy po jejich vydání, nevýhodou je, že softwarové balíčky můžou s každou novou verzí měnit své vlastnosti, a tak může dojít k rozbíjení některých komplikovanějších zřetězených funkcionalit, které požadují spolupráci vícero softwarových balíčků (typický příklad webserver využívá většinou minimálně tři softwarové balíčky – apache2, php a MySQL). Tato varianta distribuce se tedy většinou pro servery nepoužívá. Pro potřeby této práce zvolíme variantu LTS 22.04, která obsahuje verze balíčků z dubna 2022 a zaručené bezpečnostní aktualizace až do dubna roku 2027.

Stažený instalační obraz je třeba nabootovat na cílovém serveru. V případě, kdy ve firmě k instalacím operačních systémů na servery dochází často, se využívá PXE server, který serverům umožňuje z instalačního obrazu nabootovat po síti. Pokud se ale jedná pouze o jednorázovou záležitost, stačí instalační obraz vypálit na DVD, nebo rozbalit na USB flash disk. V našem případě podporuje server zavádění z USB, a tak využijeme této možnosti. Instalační obraz se na flash disk dá rozbalit pomocí příkazu dd v terminálu na operačním systému Linux, nebo programem BalenaEtcher v případě využití operačního systému Windows. Nakonec je potřeba v BIOSu serveru nastavit prioritu zavádění, kdy flash disk zařadíme v pořadí před pevný disk. Pak již jen stačí instalační flashdisk vložit do jednoho z USB portů na serveru a server restartovat.

Po zapnutí se instalátor nejdříve uživatele zeptá na jazyk, ve kterém chce systém instalovat a rozložení klávesnice, které chce používat. My samozřejmě zvolíme češtinu a české rozložení klávesnice. Jako další je volba mezi minimální a plnou instalací. Rozdíl spočívá v tom, že minimální instalace neobsahuje prakticky žádné nástroje pro konfiguraci a správu serveru. Je určena pro prostředí kde se uživatelé nebudou k serveru hlásit přímo,

ale prostřednictvím nějakého jiného nástroje pro správu. Jelikož v našem případě se budeme k serveru hlásit přímo, zvolíme variantu plné instalace.

V další sekci se instalátor věnuje konfiguraci sítě. Nejdříve zobrazí, které síťové adaptéry nalezl a dá uživateli příležitost je nakonfigurovat. Výchozí nastavení je nechat vše na DHCP, což je ale pro server nevhodné, protože v některých případech se k němu je potřeba připojit pomocí IP adresy a tehdy je lepší, když je jeho IP adresa pevná. V případě našeho serveru je dostupný pouze jeden síťový adaptér, ačkoliv server má dva, jelikož jeden z adaptérů není připojený k síti. Tomuto adaptéru je přidělena IP adresa 172.20.80.10 s maskou 255.255.252.0 a bránou 172.20.80.222. Také se zde nastavují DNS servery a doménové přípony. Jako DNS servery jsou nakonfigurovány soudní doménové řadiče s adresami 172.20.80.2 a 172.20.80.4 a jako doménová přípona a1.sou-pha.justice.cz. Tuto poslední hodnotu není nutné nastavovat, pokud není v plánu server zařazovat do domény Active Directory. Jelikož v této práci se server zařazovat bude, byla tato hodnota nastavena.

Dále se instalátor zeptá, jestli je pro připojení k internetu nutné jít přes proxy server. Instalátor totiž v průběhu instalace některé softwarové balíčky stahuje přímo z repozitářů a tak potřebuje přístup k internetu. V našem případě vyplníme hodnotu http://proxy.justice.cz:3128, což je adresa interního proxy serveru ministerstva spravedlnosti, přes který musí probíhat veškerá komunikace po internetu. Následovně instalátor ukáže odkaz na server, ze kterého bude při instalaci stahovat potřebné soubory a dá uživateli příležitost napsat adresu jiného zrcadlového serveru. My necháme výchozí možnost.

Nyní se instalátor dostává k sekci rozdělení disku. Protože server disponuje disky v hardwarovém RAID poli, z pohledu systému se jedná o jeden velký disk s velikostí 8TB. V této sekci je nutné vybrat možnost, že chceme využít celý diskový prostor a nechceme žádnou jeho část nechat nenaformátovanou, abychom tak maximalizovali prostor dostupný pro sdílené složky na síti. Instalátor nabízí možnost data na discích šifrovat. Server je bezpečně zamčen v serverové skříni v serverovně a pravděpodobnost neautorizovaného fyzického přístupu je minimální, což ve srovnání s potenciálními ztrátami výkonu kvůli využití šifrování znamená, že v našem případě šifrování nevyužijeme.

Následuje sekce pro informace o serveru a uživatelích. Zde se vyplňuje název serveru, uživatelské jméno uživatele a heslo pro uživatelský účet. V našem případě jsme zvolili název serveru SOUA1LX01 v souladu s pojmenovávací konvencí síťových prostředků pražských soudů kdy SOUA1 označuje Obvodní soud pro Prahu 1, LX označuje souborový server

s operačním systémem Linux a 01 označuje, že se jedná o první server tohoto typu v síti. Jako uživatelské jméno zvolíme „informatik“, protože se jedná o standartní uživatelské jméno pro správcovské účty zařízení mimo doménu.

Na konci nabídne instalátor možnost automaticky nainstalovat a nakonfigurovat OpenSSH server, který umožňuje se k serveru přihlásit a spravovat jej na dálku. Jelikož tuto metodu budeme v rámci práce využívat, zaškrtneme, že instalátor má instalaci provést. Poté začne samotná instalace a základní konfigurace operačního systému a softwarových balíčků. Až vše proběhne, vyzve uživatele instalátor, aby odebral instalační medium a pak stiskl enter. Server se restartuje a naběhne na přihlašovací obrazovku nově nainstalovaného operačního systému Ubuntu Server.

4.4.3 **Základní konfigurace**

Po přihlášení je nutné nastavit některé základní parametry, aby server korektně fungoval v síti. V terminálu operačního systému Linux se příkazy standartně spouštějí s oprávněními běžného uživatele a nemají možnost upravovat systémové soubory. V některých případech je příkaz nutné spustit se zvýšenými oprávněními. K tomu se používá příkaz sudo, který příkaz spustí s oprávněními superuživatele root. Nejdříve provedeme kontrolu nastavení DNS serverů, které by měl instalátor sám provést podle údajů, které uživatel zadal v průběhu instalace. Příkazem `cat /etc/resolv.conf` se do terminálu vypíše obsah tohoto souboru, který obsahuje nastavení pro DNS. V našem případě je obsah souboru následující:

```
nameserver 172.20.80.2
options edns0 trust-ad
search a1.sou-pha.justice.cz
```

Obrázek 4: Obsah souboru resolv.conf

Toto nastavení se tedy správně přeneslo z instalátoru a překládání adres na IP adresy přes doménový řadič v roli DNS serveru funguje.

Pro nastavení proxy serveru je nutné nastavit hodnoty proměnných http_proxy, https_proxy, ftp_proxy a socks_proxy na hodnotu v podobě adresy proxy serveru. K nastavení proměnných se v terminálu používá příkaz ve tvaru `export <název_proměnné>=<hodnota>`. My tedy použijeme příkazy v podobě:

```
<protokol>_proxy = http://proxy.justice.cz:3128
```

Aby tyto příkazy nebylo nutné zadávat při každém přihlášení k serveru, zapíšeme je do souboru `/etc/environment`, což zaručí, že budou nastaveny stále. Nyní je ověřeno, že server může správně přistupovat k síti a lze přistoupit k instalaci požadovaného softwaru

4.4.4 Instalace softwaru

U operačních systémů s jádrem Linux se software instaluje z oficiálních repozitářů, které spravují tvůrci dané distribuce, pomocí správců balíčků. Každá distribuce si může vybrat, kterého správce balíčků bude zahrnovat a podle této volby se odvíjí postup instalace a aktualizace softwaru. Například distribuce založené na distribuci Arch používají správce balíčků pacman, tím pádem se ke správě softwaru používá příkaz pacman. Distribuce, které jsou založeny na distribuci RHEL používají správce RPM s příkazem rpm a distribuce založené na distribuci Debian používají správce balíčků aptitude s jeho příkazem apt. Distribuce Ubuntu Server je odvozena z distribuce Debian, v našem případě tedy použijeme příkaz ve tvaru `apt install <název balíčku>`.

Než přistoupíme k instalaci balíčků, je doporučeno nejdříve všechen nainstalovaný software v systému aktualizovat. Jedná se o proces složený ze dvou kroků. První krok je stažení seznamu aktuálních dostupných verzí balíčků a druhý krok je stažení a instalování samotných aktualizací Příkazy, kterými se tyto dva kroky provedou vypadají následovně:

```
sudo apt update
sudo apt upgrade
```

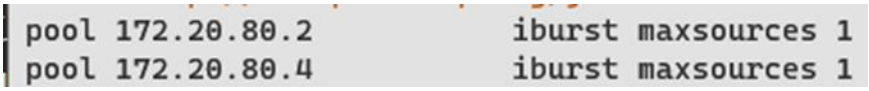
Ke sdílení složek po síti je nutné nainstalovat softwarový balíček samba a jeho doplňující části z balíčku samba-common-bin. Pro pokročilou správu oprávnění slouží balíček acl. Nástroje pro zařazení serveru do domény se nachází v balíčku realmd, služby pro autentifikaci uživatelů jsou součástí balíčků libnss-winbind libpam-winbind a winbind a nástroj umožňující synchronizaci systémového času na serveru, s časem na doménovém řadiči pomocí NTP se jmenuje chrony. Příkaz pro instalaci těchto balíčků je:

```
sudo apt install samba samba-common-bin acl realmd libnss-
winbind libpam-winbind winbind chrony
```

4.5 Zařazení do domény Active Directory

Nyní, když už je systém nakonfigurovaný a potřebné softwarové balíčky jsou nainstalovány, přišel čas zařadit server do domény. Aby členství serveru v doméně fungovalo korektně, je nutné, aby server měl stejný systémový čas, jako doménový řadič. Doménové řadiče poskytují synchronizaci času prostřednictvím protokolu NTP. V našem případě k tomuto použijeme software s názvem Chrony.

Konfigurace pro synchronizaci systémového času programem Chrony se nachází v souboru `/etc/Chrony/Chrony.conf`. Do něj je potřeba přidat dva řádky v následujícím tvaru:



Obrázek 5: Konfigurace programu Chrony

Kde pool a iburst označuje typ NTP serveru a typ komunikace, IP adresy jsou ip adresy doménových řadičů a maxsources 1 znamená, že se jedná o jednotlivé servery. Po úpravě konfiguračního souboru se provede restart služby příkazem:

```
sudo systemctl restart chrony.service
```

Příkazem date zjistíme současné nastavení systémového času, které by se již mělo shodovat se systémovým časem doménového řadiče. Synchronizace času se na první pohled může zdát nepodstatná. V kontextu domény je ale kritické, aby se čas na serveru shodoval přesně s časem na doménovém řadiči, kvůli ověřování. Při přípravě této práce byla konfigurace NTP nejdříve vynechána a pak došlo k situaci, kdy ihned po konfiguraci fungoval server přesně podle očekávání, ale o několik dní později přestal komunikovat po síti s ostatními zařízeními. Po nakonfigurování synchronizace času tento problém zmizel a znovu se již neopakoval.

Aby byl server dosažitelný v pomocí DNS názvu, musí se jeho hostname skládat z názvu serveru a doménové přípony. V Linuxových distribucích založených na debianu se hostname serveru nastavuje příkazem hostnamectl. Zadáme tedy příkaz:

```
sudo hostnamectl hostname soua1lx01.a1.sou-pha.justice.cz.
```

K zařazení serveru do domény Active Directory se u distribuce Ubuntu Server používá utilita realmd, která celý proces výrazně automatizuje. Zařazení do domény lze provést i ručním editováním řady konfiguračních souborů, ale utilita realmd toto vše provede za nás

a snižuje se tím riziko, že zařazení selže kvůli špatně vyplněné konfiguraci. Nejprve je vhodné ověřit, jestli je doména dosažitelná. Toho dosáhneme příkazem:

```
sudo realm -v discover a1.sou-pha.justice.cz
```

```
informatik@soua1lx01:~$ sudo realm discover a1.sou-pha.justice.cz
[sudo] password for informatik:
a1.sou-pha.justice.cz
  type: kerberos
  realm-name: A1.SOU-PHA.JUSTICE.CZ
  domain-name: a1.sou-pha.justice.cz
  configured: no
  server-software: active-directory
  client-software: winbind
  required-package: libnss-winbind
  required-package: winbind
  required-package: libpam-winbind
  required-package: samba-common-bin
```

Obrázek 6: Nalezené informace o doméně

Pokud máme ověřené, že server vidí doménu, můžeme začít proces zařazování do domény. Příkazem:

```
sudo realm join --membership-software=samba --client-
software=winbind a1.sou-pha.justice.cz
```

se spustí proces zařazování do domény. Příkaz se zeptá na heslo doménového uživatele Administrator a může se zeptat, jaký má být výchozí realm pro Kerberos, což v doméně active directory je doménová koncovka velkými písmeny. Nyní je server zařazen do domény a můžou s ním pracovat doménoví uživatelé. Ověřit úspěšnost zařazení do domény lze provést příkazem `getent passwd <uživatel>`, který vyhledá uživatele v doméně a ukáže nalezené informace. Pokud by v komunikaci s doménou byl nějaký problém, tento příkaz nevrátí žádnou hodnotu. Samozřejmě že hledaný uživatel musí v doméně opravdu existovat, proto se doporučuje do příkazu getent použít uživatele Administrátor, který je automaticky vytvořen v každé doméně Active Directory. Active Directory používá pro oddělení názvu domény od uživatelského jména jako znak zpětné lomítko \, které se v terminálu používá jako únikový znak. Kvůli tomu je při používání doménových

uživatelských jmen a skupin v příkazech buď toto lomítko napsat dvakrát, nebo celý argument zapsat v uvozovkách:

```
informatik@soua1lx01:~$ getent passwd SOUA1\\Administrator
SOUA1\administrator:*:2000500:2000513::/home/administrator@SOUA1:/bin/bash
```

Obrázek 7: Výsledek příkazu getent

Pokud je žádoucí, aby se k serveru mohli doménoví uživatele přihlašovat i pomocí protokolu SSH, nebo lokálního terminálu, musí jim být při prvním přihlášení vytvořena domovská složka. U distribuce Ubuntu je tato funkce ve výchozím nastavení deaktivovaná, aktivaci lze provést příkazem:

```
sudo pam-auth-update --enable mkhomedir
```

Jelikož v našem případě se bude v budoucnu o administraci serveru starat více správců, tuto možnost zapneme. Když se na server s operačním systémem Windows Server, připojí uživatel, který je ve skupině doménových administrátorů, jeho účet má na serveru automaticky přidělenou hodnost administrátor a může provádět akce se zvýšenými oprávněními. Aby analogicky doménoví administrátoři dostali na Linuxovém serveru oprávnění spouštět příkazy se zvýšenými oprávněními pomocí příkazu sudo, je nutné do souboru `/etc/sudoers` přidat řádek v podobě:

```
%SOUA1\\domain\ admins ALL=(ALL:ALL) ALL.
```

4.6 Konfigurace sdílených složek

4.6.1 Založení nové sdílené složky

Nyní je server plnohodnotným členem domény Active Directory. Může komunikovat s doménovým řadičem a ověřovat uživatele a zároveň na něj lze přistupovat z počítačů, které jsou také členy domény. Když se na něj někdo pokusí připojit pomocí protokolu SMB, neuvidí ale nic, jelikož na serveru ještě nejsou nastavené žádné sdílené složky.

Pro využívání serveru bude vytvořeno několik sdílených složek, podle počtu jednacích síní na soudu. Jelikož konfigurace každé z těchto složek bude totožná, s výjimkou čísla jednací síně, bude zde popsána jen konfigurace složky pro jednací síň číslo 126. Nejdříve je nutné složku vytvořit. Není vhodné tuto složku vytvářet v rámci domovské složky některého z uživatelů, jelikož může docházet ke konfliktům ohledně vlastnictví složky a přístupových

práv. Proto bude v kořenovém adresáři serveru vytvořena složka `/srv`, ve které budou uloženy jednotlivé složky ke sdílení. Právo na tvorbu složek v kořenovém adresáři má pouze uživatel root a proto příkaz pro vytvoření složky spustíme pomocí programu `sudo`. Příkaz tedy bude vypadat takto: `sudo mkdir /srv`. Následovně vytvoříme jednotlivé složky příkazem `sudo mkdir /srv/js126`. Aby složku mohli spravovat doménoví administrátoři, nastavíme jako vlastníka doménového uživatele Administrator, a doménovou skupinu domain admins. Toho dosáhneme příkazem:

```
sudo chown "SOUA1\Administrator":"SOUA1\domain admins"
/srv/js126
```

Pokud nebudou uživateli nebo skupině jmenovitě přiřazena oprávnění, neměl by uživatel mít ke složce vůbec přístup. Proto nastavíme přístupová práva vlastníka (uživatele a skupiny) na úplné řízení a ostatním uživatelům práva kompletně odebereme. K tomu se využije příkaz chmod v následující podobě:

```
sudo chmod 0770 /srv/js126
```

Konfigurace softwaru Samba je uložena v souboru `/etc/samba/smb.conf`, budou se zde tedy nastavovat i sdílené složky. Do souboru byly softwarem realmd zapsány konfigurační údaje, které slouží ke komunikaci s doménou Active Directory. Tyto údaje tedy nebudeme manuálně měnit, jelikož zapojení do domény již máme otestováno jako funkční. Jelikož server bude fungovat s oprávněními uživatelů Active Directory, je potřeba aktivovat podporu oprávnění typu ACL a jejich dědičnost. K tomu složí dvojice konfiguračních příkazů, které je nutné do souboru smb.conf přidat. Jedná se o příkazy:

```
map acl inherit = Yes
vfs objects = acl_xattr
```

Tyto příkazy umožní sambě ukládat v rozšířených vlastnostech souborů přístupová oprávnění typu Windows ACL, což umožní přidělovat oprávnění zvlášť každému uživateli a skupině v doméně.

Na konci souboru je v komentáři zapsaná ukázková konfigurace sdílené složky v podobě názvu sdílené složky v hranatých závorkách, a vlastností, jako je například cesta ke složce na disku serveru, možnost nastavit složku jen pro čtení a volitelný komentář, v podobě řádkových příkazů pod názvem složky. Na základě této šablony vytvoříme na konci souboru nový záznam pro novou sdílenou složku.

```
[js126]
        comment = Jednaci Sin 126
        path = /srv/js126
        read only = No
```

Obrázek 8: Záznam sdílené složky v souboru smb.conf

Po editaci konfiguračního souboru softwaru Samba je doporučeno spustit ověřovací příkaz `testparm`, který soubor zkontroluje a v případě chybné syntaxe ukáže, kde se chyba nachází. Pokud je konfigurační soubor správný, je nutné, aby si Samba tento nově změněný konfigurační soubor načetla. Jednou z možností, jak toho dosáhnout je restart Samby, což ale způsobí dočasný výpadek dostupnosti existujících sdílených složek, což je nežádoucí. Samba proto pro tyto účely obsahuje příkaz pro znovunačtení konfigurace ve formě:

```
sudo smbcontrol all reload-config
```

Po spuštění tohoto příkazu je nově sdílená složka přístupná uživateli Administrator, nebo členům skupiny domain admins, z jakékoliv pracovní stanice na síti na adrese \\soua1lx01\js126

4.6.2 Konfigurace přístupových práv v operačním systému Linux

Přidělování oprávnění pro doménové uživatele a skupiny probíhá zápisem do rozšířených atributů souboru nebo složky. V Linuxu se k tomuto používá balíček acl a jeho dva příkazy `getfacl` a `setfacl`. Getfacl slouží ke čtení ACL oprávnění souboru a setfacl k jejich zapisování a editování.

Námi vytvořená sdílená složka v současnosti nemá přidělená žádná speciální přístupová práva, pouze základní Unixová práva pro vlastníka, skupinu a ostatní. Ačkoliv uživatelé, kteří nemají přístup je složce jmenovitě přidělený přes atributy ACL, již mají přístup ke složce a jejím souborům zakázaný pomocí Unixových přístupových oprávnění, nově vytvořené soubory toto nastavení nerespektují, a tak by k nim mohli přistupovat i neoprávnění uživatelé. Proto je nutné v ACL nastavit práva pro složku, která budou nově vytvořené soubory dědit. Dědičná práva se v ACL nastavují podobně jako normální práva, jen se před specifikaci uživatele nebo skupiny napíše default. Příkazem:

```
sudo setfacl -m default:group::--- /srv/js126
```

nastavíme přístupová práva pro nově vytvořené soubory tak, že uživatelé bez oprávnění ke sdílené složce k nim nebudou moci přistupovat.

V našem případě potřebujeme uživateli jednací síně přidělit práva pro úplné řízení a zapisovatelkám civilního úseku práva pro čtení a spouštění. K tomuto využijeme dva příkazy getfacl v těchto formách:

```
sudo setfacl -m user:"SOUA1\js126":rwx /srv/js126
sudo setfacl -m group:"SOUA1\_Zapisovatelky civil":r-x
/srv/js126
```

Aby tato oprávnění zdědily i nově tvořené soubory ve sdílené složky, příkazy zopakujeme s klíčovým slovem default:

```
sudo setfacl -m default:user:"SOUA1\js126":rwx
/srv/js126
sudo setfacl -m default:group:"SOUA1\_Zapisovatelky
civil":r-x /srv/js126
```

Nyní můžeme příkazem sudo getfacl /srv/js126 zkontrolovat jaké atributy jsou na složku aplikovány:

```
informatik@soua1lx01:~$ sudo getfacl /srv/js126/
getfacl: Removing leading '/' from absolute path names
# file: srv/js126/
# owner: SOUA1\\administrator
# group: SOUA1\\domain\040admins
user::rwx
user:SOUA1\\js126:rwx
group::rwx
group:SOUA1\\_zapisovatelky\040civil:r-x
mask::rwx
other::---
default:user::rwx
default:user:SOUA1\\js126:rwx
default:group::---
default:group:SOUA1\\_zapisovatelky\040civil:r-x
default:mask::rwx
default:other::---
```

Obrázek 9: Seznam rozšířených atributů složky

4.6.3 Konfigurace přístupových práv v operačním systému Windows

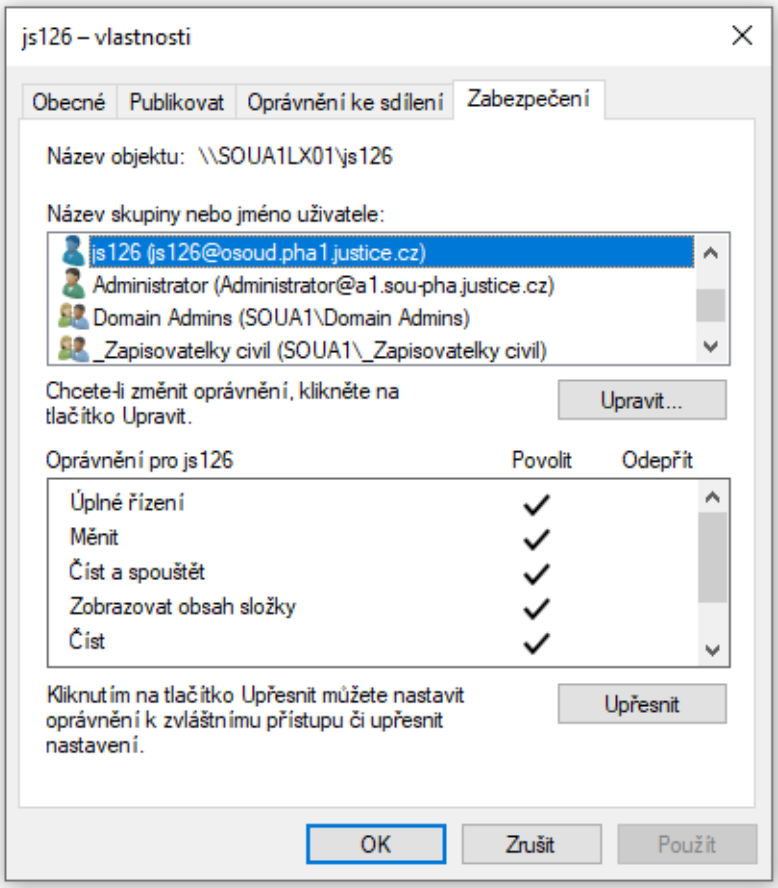
Pro zjednodušení správy přístupových práv administrátorům, kteří preferují grafická uživatelská rozhraní před příkazovou řádkou, nabízí samba možnost spravovat přístupová

práva sdílených složek pomocí nástrojů pro správu operačního systému Microsoft Windows. Aby mohl doménový uživatel sdílené složky na severu spravovat, musí mít na serveru přiděleno oprávnění SeDiskOperatorPrivilege. Toto oprávnění lze přidělit jednotlivým uživatelům, nebo skupinám v doméně. Aby oprávnění sdílených složek mohl spravovat kdokoliv z doménových administrátorů, přidělíme oprávnění SeDiskOperatorPrivilege skupině domain admins. Příkaz bude vypadat takto:

```
net rpc rights grant "SOUA1\domain admins"
SeDiskOperatorPrivilege -U "SOUA1\administrator"
```

Kde SOUA1\administrator je doménový administrátorský účet, jehož jménem je oprávnění přiděleno. Po zadání příkazu je uživatel vyzván k zadání hesla tohoto administrátorského účtu.

Nyní může kterýkoliv člen skupiny domain admins na pracovní stanici s operačním systémem Microsoft Windows otevřít nástroj správa počítače, vybrat možnost „Připojit k jinému počítači“, do kolonky pro název počítače napsat název serveru (v našem případě SOUA1LX01) a odtud provádět správu sdílených složek na Linuxovém souborovém serveru, zobrazovat a rušit relace a zobrazovat seznam otevřených souborů uživateli. Ve vlastnostech sdílené složky se nachází několik záložek s nastaveními. První z nich je záložka obecné, která umožňuje nastavit základní informace o složce, jako její název, popis a umístění. Změna těchto hodnot se přímo propíše do konfiguračního souboru smb.conf na disku serveru. Záložka publikovat obsahuje možnosti pro publikování sdílené složky v adresáři Active Directory. Touto funkcí lze odkaz na sdílenou složku uložit jako objekt v adresáři a díky tomu ji lze lépe vyhledat. Poslední dvě záložky – oprávnění ke sdílení a zabezpečení zajišťují správu přístupových práv. Jedná se o dva nezávislé seznamy uživatelů, kteří mají oprávnění přistupovat ke složce. Výsledný seznam oprávnění uživatelů se získá průnikem těchto dvou seznamů. V případě Linuxového souborového serveru je na seznamu v záložce oprávnění ke sdílení pouze položka everyone, která má přidělena práva k plnému řízení. Seznam na záložce zabezpečení zobrazuje uživatele a oprávnění, která jsou u složky na souborovém serveru zapsány v rozšířených atributech ACL:



Obrázek 10: Správa oprávnění sdílené složky v OS Windows

4.7 Testování

Po nakonfigurování sdílených složek a přístupových oprávnění je vhodné otestovat, jestli se souborový server chová podle očekávání. Pro otestování použijeme několik různých uživatelských účtů s různými druhy oprávnění.

První profil použitý k testování je profil SOUA1\administrator, který patří do skupiny SOUA1\domain admins. Tento uživatel a skupina jsou vlastníky sdílené složky a podle nastavení oprávnění na serveru by měli mít plný přístup ke složce. Další profil využitý k otestování je profil SOUA1\js126, kterému byla pomocí rozšířených atributů ACL přidělena oprávnění k úplnému řízení složky. Profil soua1\zapisove patří do skupiny SOUA1_Zapisovatelky, a tak by podle přidělených oprávnění měl mít právo číst obsah sdílené složky, ale přístup k zápisu by mu měl být zamítnut. Poslední profil použitý k testování je SOUA1\brigada, který nemá ke sdílené složce přidělená žádná oprávnění, a tak by mu veškeré operace se složkou – čtení, i zápis, měly být zamítnuty. Výsledky testování jsou zapsány v následující tabulce:

Doménový Uživatel	Zdroj oprávnění	Typ přístupu	Očekáváný výsledek	Pozorovaný výsledek
Administrator	Vlastník	Čtení	Přístup povolen	Přístup povolen
Administrator	Vlastník	Zápis	Přístup povolen	Přístup povolen
js126	ACL – Uživatel	Čtení	Přístup povolen	Přístup povolen
js126	ACL – Uživatel	Zápis	Přístup povolen	Přístup povolen
zapisove	ACL – Skupina	Čtení	Přístup povolen	Přístup povolen
zapisove	ACL – Skupina	Zápis	Přístup zamítnut	Přístup zamítnut
brigada	-	Čtení	Přístup zamítnut	Přístup zamítnut
brigada	-	Zápis	Přístup zamítnut	Přístup zamítnut

Tabulka 1: Výsledky testování přístupových oprávnění

5 Výsledky a diskuse

5.1 Výsledek práce

Výsledkem této bakalářské práce je plně funkční souborový server komunikující prostřednictvím protokolu SMB. Použitý software se odvíjel od předem zvolených požadavků. Požadavek na operační systém Linux s nejnovějšími bezpečnostními záplatami byl splněn instalací Linuxové distribuce Ubuntu LTS 22.04. Disky byly spojeny díky RAID řadiči serveru spojeny do diskového pole RAID 5, čímž byly splněny požadavky na spojení disků do diskového pole, a požadavky na odolnost pole proti selhání disku. Server byl prostřednictvím softwarových balíčků Samba a Winbind zařazen do domény a softwarový balíček Samba byl také využit ke sdílení složek prostřednictvím protokolu SMB. Díky zařazení do domény bylo možné jednotlivým doménovým uživatelům a skupinám přidělit oprávnění ke sdíleným složkám.

5.2 Diskuse

V současnosti je podpora Linuxových serverů v doménách Active Directory na velmi dobré úrovni, kdy pro většinu reálných využití je funkcionalita serveru s operačním systémem Windows Server a Linux totožná. Vzniká otázka, zda v případě větších změn, ve fungování domén Active Directory, ze strany společnosti Microsoft, dokáže open-source komunita dostatečně rychle zareagovat, aby funkcionalita Linuxových serverů v doméně byla zachována.

Další otázkou je relevance čistě Linuxového souborového serveru v době, kdy se ve firemních serverovnách čím dál tím častěji objevují dedikované NAS stroje, které jsou za účelem sdílení složek stvořeny a mají k tomu svůj vlastní operační systém, který je sice založený na Linuxu, ale je pro účely zařazení do domény a sdílení složek předem nakonfigurovaný, a síťovému administrátorovi tak odpadá veškerá práce s instalací operačního systému, potřebných softwarových balíčků a jejich konfigurací.

6 Závěr

Cílem práce bylo nainstalovat a nakonfigurovat souborový server na operačním systému Linux a zařadit jej do domény. Byla nainstalována Linuxová distribuce Ubuntu LTS kvůli dostupné rozsáhlé dokumentaci, softwarových balíčcích v repozitářích, dlouhodobé podpoře a stabilitě. Pro synchronizaci času s doménovým řadičem byl použit softwarový balíček Chrony. Zařazení do domény proběhlo prostřednictvím softwarových balíčků Samba a Winbind. Ke konfiguraci zařazení serveru do domény byla použita utilita Realmd. Pro sdílené složky byl využit protokol SMB prostřednictvím softwarového balíčku Samba.

Instalace byla provedena na serveru v síti Obvodního Soudu pro Prahu 1. Nejdříve byl jako DNS server nastaven doménový řadič, poté byla nakonfigurována synchronizace času serveru s doménovým řadičem přes protokol NTP, čímž byla vyřešena situace, kdy po desynchronizaci času mezi doménovým řadičem a serverem přestal server komunikovat po síti. Server byl zařazen do domény Active Directory a funkčnost komunikace byla otestována. Nakonec byly nakonfigurovány sdílené složky a uživatelům domény byly přiděleny přístupová oprávnění k těmto složkám, a to pomocí příkazové řádky přímo na serveru i vzdáleně z pracovní stanice s operačním systémem Windows.

Výsledkem práce je plně funkční souborový server běžící na operačním systému Linux zařazený v doméně Active Directory, přístupný oprávněným uživatelům na síti. Hlavním přínosem této práce je využití starého serveru, který již nepodporuje nové verze operačního systému Windows Server a používání starých verzí je bezpečnostním rizikem a je tedy v síti obvodního soudu nepřípustné. I když je server již technologicky zastaralý pro novější verze operačního systému, je stále plně funkční a dostačující pro potřeby středně vytíženého souborového serveru. Tato práce umožňuje efektivní využití stávající infrastruktury a minimalizuje náklady spojené s nákupem nového hardware.

7 Seznam použitých zdrojů

BOUŠKA, Petr. 2008. Active Directory komponenty – domain, tree, forest, site. [online]. Samuraj-cz. [cit. 2024-02-08]. Dostupné z: https://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/.

BOUŠKA, Petr. 2007. Adresářové služby a LDAP. Samuraj-cz [online]. [cit. 2024-02-08]. Dostupné z: https://www.samuraj-cz.com/clanek/adresarove-sluzby-a-ldap/

BOUŠKA, Petr. 2014. Kerberos část 2 - AD uživatelské účty a Service Principal Name. Samuraj-cz [online]. [cit. 2024-02-08]. Dostupné z: https://www.samuraj-cz.com/clanek/kerberos-cast-2-ad-uzivatelske-ucty-a-service-principal-name/

CZ.NIC. 2017. Doména, IP adresa, DNS. Jak na internet [online]. [cit. 2024-02-10]. Dostupné z: https://www.jaknainternet.cz/page/1261/domena,-ip-adresa,-dns/

HERTEL, Christopher. 2003. Implementing CIFS: The Common Internet File System. Prentice Hall, ISBN 013047116X.

MICROSEMI. 2017. Hardware RAID vs. Software RAID: Which Implementation is Best for my Application? [online]. [cit. 2024-02-10]. Dostupné z: https://ww1.microchip.com/downloads/en/DeviceDoc/Hardware_RAID_vs_Software_RAID__Which_Implementation_is_Best_for_my_Application_Whitepaper.pdf

MICROSOFT CORPORATION. 2009. Active Directory Architecture. Microsoft Learn [online]. [cit. 2024-02-08]. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727030(v=technet.10)?redirectedfrom=MSDN

MICROSOFT CORPORATION. 2012. Common Internet File System. Microsoft Learn [online]. [cit. 2024-02-08]. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc939973(v=technet.10)

MICROSOFT CORPORATION. 1993. Microsoft® Windows Cairo Product Planning: Product Requirements. Dostupné také z: https://web.archive.org/web/20120925132235/http://antitrust.slated.org/www.iowaconsumercase.org/011607/5000/PX05542.pdf

MŮČKA, Jan. 2021. RAID disková pole: jaké jsou základní typy a v čem se liší? MasterDC [online]. [cit. 2024-02-10]. Dostupné z: https://www.master.cz/blog/raid-diskova-pole-jake-jsou-zakladni-typy-a-v-cem-se-lisi/

SITERA, Jiří. 2000. Adresářové služby – úvod do problematiky. Archiv cesnet [online]. [cit. 2024-02-08]. Dostupné z: https://archiv.cesnet.cz/doc/techzpravy/2000-4/

SVIDERGOL, Brian. 2017. Evolution of Windows Domain Controller. [online]. Netwrix. [cit. 2024-02-08]. Dostupné z: https://blog.netwrix.com/2017/01/30/evolution-of-windows-domain-controller/.

ŠULC, Tomáš. 2008. VelociRaptory a RAID – když jeden nestačí. Pctuning [online]. [cit. 2024-02-10]. Dostupné z: https://pctuning.cz/article/velociraptory-a-raid-kdyz-jeden-nestaci

THURROTT, Paul. 1999. The Road to Gold: The development of Windows 2000 Reviewed. Paul Thurrott's SuperSite for Windows [online]. [cit. 2024-02-08]. Dostupné z: https://web.archive.org/web/20000816180054/http://www.winsupersite.com/reviews/win2k_gold.asp

THURROTT, Paul. 2000 .Windows 2000 Server Beta 3 Reviewed. Paul Thurrott's SuperSite for Windows [online]. [cit. 2024-02-08]. Dostupné z: https://web.archive.org/web/20001022085730/http://www.winsupersite.com/reviews/win2k_server_b3.asp

TRANQUIL IT. 2023. History of Samba Active Directory. Samba-AD documentation [online]. [cit. 2024-02-08]. Dostupné z: https://samba.tranquil.it/doc/en/samba_fundamentals/samba_history.html

TRIDGELL, Andrew. 2002. 10 years of Samba! [online]. [cit. 2024-02-08]. Dostupné z: https://www.samba.org/samba/docs/10years.html

TRIDGELL, Andrew. 1994. A bit of history and a bit of fun. Online. Samba. [cit. 2024-02-08]. Dostupné z: http://ftp.samba.org/ftp/unpacked/samba/docs/history.

ZAPLETAL, Lukáš. 2000. Lehký úvod do LDAP. Root.cz [online]. [cit. 2024-02-08]. Dostupné z: https://www.root.cz/clanky/lehky-uvod-do-ldap/

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam použitých zkratek

ACL – Access Control List

AD - Active Directory

DC - Domain Component

DN - Distinguished name

DNS - Domain Name Systém

GUID - Globally Unique Identifier

JBOD - Just a Bunch of Disks

LDAP - Lightweight Directory Access Protocol

NTLM - NT Lan Manager

NTP - Network Time Protocol

OU - Organizational Unit

RAID - Redundant array of independent disks

RDN - Relative Distinguished Name

SAM - Security Account Manager

SASL - Simple Authentication and Security Layer

SID - Security Identifier

SMB - Server message block

TCP/IP - Transmission Control Protocol / Internet Protocol