Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Datové úložiště pro potřeby JU

Bakalářská práce

František Kubeš, DiS.

Vedoucí práce: Mgr. Miloš Prokýšek, Ph.D.

České Budějovice 2014

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL BAKALÁŘSKÉ PRÁCE

Student: František Kubeš, DiS.

Obor – zaměření studia: Měřicí a výpočetní technika

Katedra: Ústav fyziky a biofyziky

Školitel: Milan Předota, RNDr., Ph.D.

Školitel – specialista, konzultant: Josef Milota, RNDr.

Téma bakalářské práce: Datové úložiště pro potřeby JU

Cíle práce :

Cílem práce je najit vhodné datové úložiště pro potřeby zaměstnanců JU dostupného ze sítě internet . V práci se student zaměří na problematiku dostupnosti a bezpečnosti dat a dále na uživatelsky přívětivý přístup. Student v práci provede komparativní analýzu jednotlivých řešení a provede experimentální implementaci v prostředí JU.

Základní doporučená literatura :

Financování práce :.....

Vedoucí práce : Miloš Prokýšek, Mgr., Ph.D. .....podpis :.....

U externích vedoucích fakultní garant práce.....podpis : .....

Vedoucí katedry: RNDr. Milan Předota, Ph.D. ..... podpis: .....

V Českých Budějovicích dne ....4.1.2013.....

Převzal/a dne.....4.1.2013..... podpis : .....

Kubeš, F., 2014: Datové úložiště pro potřeby JU
[The datastorage for the university needs. Bc.. Thesis, in Czech.] - 49 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic

Anotace

Tato práce pojednává o implementaci inovace do datového úložiště pro potřeby zaměstnanců JU, která zvýší dostupnost z vnější sítě JU a umožní automatickou synchronizaci dat mezi koncovým zařízením a tímto úložištěm, se zaměřením na uživatelsky přívětivý přístup.

Abstract

This thesis deals with implementation of innovation of data storage for the needs of employees JU, which would increase the availability of JU external networks and would enable automatic synchronization of data among endpoint devices and this data store, with a focus on user-friendly approach.

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

Drahotěšice, 24. 4. 2014

František Kubeš, DiS.

Poděkování

Rád bych touto cestou vyjádřil poděkování Mgr. Miloši Prokýškovi, Ph.D. za jeho cenné rady a trpělivost při vedení mé bakalářské práce, Ing. Ondřejovi Ševečkovi za konzultaci problematiky offline files a své ženě za podporu a pochopení, nejen při psaní bakalářské práce.

Obsah

1. Úvod

Čím dál častěji se setkáváme s požadavkem, kdy uživatelé chtějí mít svá data synchronizovaná mezi svými zařízeními, zálohovaná a samozřejmě dosažitelná z internetu. A to vše musí probíhat automaticky „samo“ s ohledem na bezpečnost těchto, kolikrát velmi citlivých a cenných dat.

Pokud se jedná o jednotlivé osoby, či malé organizace, většinou spoléhají na komerční programy dostupné v internetu. Tyto programy dávají obvykle úložný prostor v podobě několika jednotek gigabytů zdarma. Pokud uživatel potřebuje tento prostor zvětšit, pak je mu to nabídnuto za pravidelný měsíční paušál.

U větších organizací, které mají datová centra, převážně můžeme najít vlastní řešení. Ta jsou závislá na základní softwarové vybavenosti organizace a na tom jak je provedena synchronizace koncových stanic s úložištěm.

1.1. Formulace problému

Vývoj informatiky v oblasti ukládání dat do internetu a synchronizací mezi různorodými platformami se vyvíjí velmi rychle. Na trhu se nachází mnoho softwarových řešení, ať už placených nebo verzí zdarma. Každé je ovšem svým způsobem jiné a vhodné pro jiný způsob používání, ať už mluvíme o vlastní konstrukci programu, nebo o licenčních podmínkách použití, které jsou nedílnou součástí řešení komerčních i bezplatných.

V prostředí JU je tento požadavek již delší dobu, avšak kvůli decentralizaci jednotlivých pracovišť je velmi obtížné vytvořit řešení, které by mohlo být masově použito především na čím dál více se rozrůstající základnu přenosných zařízení a tím sekundárně vyřešit i jejich zálohování. V současné době není neobvyklé, aby jeden uživatel měl více než jedno zařízení. Pak nastává otázka, jak synchronizovat data z jednoho na druhé a udržovat je na všech vždy v aktualizované podobě. To samé platí i o jednotlivých pracovištích, kde je požadavek na sdílené složky mezi několika uživateli, kteří sdílejí velká množství dat.

1.2. Výzkumné otázky

1) Vyplatí se řešit datové úložiště?

2) Jaké jsou přínosy, jaké jsou negativa?

3) Jaká je bezpečnost dat v případě jejich uložení do cloud služeb?

1.3. Cíl práce

Hlavním cílem práce je analyzovat a nasadit do centrální sítě Active Directory JU (ad.jcu.cz) funkci offline files, která bude zároveň nasměrována na současná vlastní datová úložiště součástí JU, začleněních do ad.jcu.cz, čímž zajistíme zvýšenou variabilitu použitelnosti stacionární i přenosné techniky založené na podporované platformě Microsoft Windows. Před vlastní analýzou a nasazením této funkce porovnám několik bezplatných webových úložišť používaných na JU a vyhodnotím je na modelové situaci.

1.4. Úkoly pro dosažení cíle

Na začátku bych chtěl analyzovat několik bezplatných webových úložišť (Dropbox, Google Drive a SkyDrive – nově OneDrive) používaných v prostředí JU, porovnat jejich použitelnost z hlediska právních aspektů a vyhodnotit je na modelové situaci. Následně implementuji offline files do ad.jcu.cz a popíši její princip.

1.5. Použité nástroje a metody

Při plnění úkolů je využito jak stacionárních, tak přenosných zařízení založených na platformě Microsoft Windows. Výsledný produkt je testován v doménových i nedoménových sítích JU a v sítích vně JU s připojením VPN JU.

Pro ověření závěru v první části bude využito modelové situace a též provedu porovnání z hlediska použitelnosti právních aspektů. V druhé části zhodnotíme konfiguraci offline files v prostředí ad.jcu.cz.

2. Cloud computing

V současné době lze v prostředí JU použít k přenosu dat email (v případě menších souborů), u větších množství dat internetovou úschovnu (např. http://www.ulozto.cz, http://www.uschovna.cz, http://www.leteckaposta.cz, http://www.edisk.cz), nebo v lepším případě některá fakultní řešení (FTP servery, WebDAV, VPN+SMB, atd.), která ovšem pro svou činnost vyžadují připojení k internetu. Emaily se k účelu přenosu dat nehodí už z toho hlediska, že mají omezenou kapacitu na počet a velikost souborů v příloze, obvykle to bývá 15-20MB. Nehledě na to, že díky těmto výměnám dat rapidně rostou emailové schránky, čímž vznikají další problémy. Výměna dat pomocí internetových úschoven je vhodná, avšak neřeší problém s archivací dat, protože bez zakoupení prémiových služeb mají omezenou dobu skladování souborů.

Z hlediska zachování uživatelsky přívětivého přístupu by bylo nejlepší, aby měl uživatel v tomto řešení veškerá svá data. Avšak zde začneme narážet na různé technické hranice, u kterých víme, že je nebudeme moci splnit všechny. Vezmeme-li např. v úvahu, že bychom měli v tomto řešení všechna data obsažená v přenosném zařízení tak, aby v situaci, kdy o toto zařízení s daty přijdeme, budeme mít ještě někde na serveru všechna jeho data. To se v dnešní době může stát velmi lehce, nemám na mysli situaci, kdy nám dané zařízení někdo ukradne, ale především v nových tenkých přenosných zařízeních jsou integrovány velmi rychlé SSD disky, které v případě havárie sebe sama prakticky nedávají naději na obnovu dat. Jenže ať už použijeme jakýkoliv nástroj, bude to dobré do doby, než narazíme na poštu, či databáze. Při otevření pošty (v případě pop3) budeme mít na disku poměrně velké otevřené soubory, což by znamenalo, že při každé změně, či následném zavření poštovního klienta (v otevřeném stavu se těmito soubory nedá manipulovat) by musela začít migrace těchto nemalých souborů (není výjimkou, že tyto soubory mají až několik jednotek GB) a tudíž by se nám velmi zhoršila práce s nahráváním do cloudu.

2.1. Dropbox

Dropbox se datuje od roku 2007, kdy ho založili dva studenti, Arash Ferdowsiem a Drew Houstonem.[1]

Toto je jedna z nejznámějších služeb, která se zde ujala a také se tu těší velké oblibě vzhledem ke své jednoduchosti, bohužel nemá českou lokalizaci. Pro nainstalování agenta nám stačí krátká registrace na stránkách https://www.dropbox.com, která je podmíněná, jako každá služba vložením naší emailové adresy. V základu máme na výběr, budeme-li chtít použít bezplatný prostor 2GB a nebo placený, za měsíční paušál viz tabulka. U této služby máme ještě další volbu v podobě plnění různých úkolů a tím získat navíc pár stovek MB, např. nalákat dalšího uživatele a tím získat 500MB, maximálně však 16GB[2].

Tabulka 1 Cena prostoru u služby Dropbox[3]

Velikost	2GB	100GB	200GB	500GB
Cena/měsíc	Zdarma	$9.99	$19,99	$49,99

Ještě bych chtěl upozornit na adresu http://www.dropbox.cz, což je sice podobná služba, avšak placená, v ceníku naleznete nejzákladnější 100MB balíček pro 10 uživatelů za roční poplatek 15.000,-.[4]

Po instalaci agenta a následném přihlášení definujeme cestu na cílový adresář, kde se vytvoří cílová složka. Výchozí cesta pro data je C:\Users*user*\Dropbox a pro cache C:\Users*user*\Dropbox\.dropbox.cache

Po instalaci a definování výchozí cesty, můžeme začít nahrávat data do složky Dropbox, automaticky se vše začne synchronizovat s webovým úložištěm. Synchronizace je prováděna na základě porovnávání časových razítek mezi

[1] Dropbox. Wikipedia [online]. 2013 [cit. 2014-04-19]. Dostupné z: http://cs.wikipedia.org/wiki/Dropbox
[2] Get more space. Dropbox [online]. 2014 [cit. 2014-2-5]. Dostupné z: https://www.dropbox.com/getspace
[3] Upgrade to Dropbox Pro. Dropbox [online]. 2014 [cit. 2014-03-04]. Dostupné z: https://www.dropbox.com/upgrade
[4] DropBox. DropBox [online]. 2014 [cit. 2014-03-04]. Dostupné z: http://www.dropbox.cz/web/cenik-programy.html

webovým úložištěm a lokálním adresářem. Přenos souborů je šifrován 256-bit SSL, samotné uložení dat používá algoritmus AES-256 standard, což je poměrně silné zabezpečení.[1]

Při používání této služby je třeba zdůraznit několik aspektů, které jsou velmi důležité. Pokud používáme službu zdarma, máme k dispozici tlačítko „Předchozí verze“, kdy si můžeme obnovit např. smazaný soubor. Avšak pokud používáme službu placenou, 100GB, 200GB, 500GB setkal jsem se v praxi s tím, že tato služba nebyla aktivní. Bohužel jsem o tomto problému nikde v dostupných materiálech nenašel jedinou zmínku.

Dalším menším nedostatkem je používání v doménových veřejných učebnách, kde je nastaveno mazání profilů uživatelů po odhlášení. Toto je základní politika na veřejných zařízeních, aby nedocházelo k odčerpávání použitelného místa na disku. V tomto případě uživatel nainstaluje agenta do zařízení, který se nainstaluje právě do profilu, vše běží, ale po odhlášení se mu profil i s agentem smaže, a z důvodu překročení kvóty (sám agent má velikost od 73MB), se mu všechna data nedopropagují na datové pole. Tím pádem přijdeme jak o agenta, tak hodnotu registru uživatele a po následném přihlášení, třeba na tom samotném počítači agent nenaběhne. Proto je vhodné na toto myslet již v počátku a používají-li uživatelé v dané lokalitě tuto službu, koncipovat zařízení na učebnách při stavbě zásad zabezpečení pro tyto případy.

Při analýze použitelnosti z hlediska právních aspektů u této služby je nutno upozornit na jeden odstavec týkající se ukončení služby.[5]

„You're free to stop using our Services at any time. We also reserve the right to suspend or end the Services at any time at our discretion and without notice. For example, we may suspend or terminate your use of the Services if you're not complying with these Terms, or use the Services in a manner that would cause us legal liability, disrupt the Services or disrupt others' use of the Services. Except for Paid Accounts, we reserve the right to terminate and delete your account if you

[5] Terms of Service. Dropbox [online]. 2014 [cit. 2014-03-25]. Dostupné z: https://www.dropbox.com/terms#terms

haven't accessed our Services for 12 consecutive months. We'll of course provide you with notice via the email address associated with your account before we do so.“

2.2. Google Drive

Tato služba je datována od roku 2012[6]. Při vzniku čerpali její autoři ze služeb jako je Dropbox, SkyDrive, které už v tu dobu byly na trhu poměrně delší dobu a měli své funkce odladěné. Jejím nesporným kladem je pro mnoho uživatelů česká lokalizace a implementace s různými službami: Google Docs, Google Drawings, Gmail, Kalendář, Google+, atd. Pokud jsme již registrováni a u společnosti Google vlastníme účet, další registrace již není nutná. Pokud ji nemáme, vytvoříme si ji zde http://drive.google.com, po ní následuje opět stažení synchronizačního klienta a vytvoření cílové složky. Nespornou výhodou jsou integrované komponenty ve webovém rozhraní této služby. Lze zde vytvářet a editovat dokumenty, aniž bychom měli nainstalovaný na daném počítači jakýkoliv jiný textový editor, samozřejmostí je i kreslení, vytváření tabulek, prezentací, konverze mezi formáty nebo spolupráce několika lidí v reálném čase na jednom projektu. Pokud začneme porovnávat ostatní produkty, zjistíme, že přejaté funkce a vzhled je právě od dvou největších rivalů na současném trhu a to právě služby OneDrive a Dropbox. Za zmínku stojí i propojení se službou Google Picasa a implementovaného rozpoznávání obličejů na našich fotografiích.

Základní prostor byl ještě nedávno na hranici 5GB, vzhledem k neustálým změnám je v současné době základní prostor stanoven na 15GB[7]. Samozřejmostí je možnost navýšení základního prostoru za stanovený měsíční paušál, viz tabulka.

Tabulka 2 Cena prostoru u služby Google Drive[7]

Velikost	15GB	100GB	1TB	10TB	20TB	30TB
Cena/měsíc	Zdarma	$1,99	$9,99	$99,99	$199,99	$299,99

[6] Google Drive. Wikipedia [online]. 2012 [cit. 2014-1-2]. Dostupné z: http://en.wikipedia.org/wiki/Google_Drive

[7] Storage Plan Pricing. Support Google [online]. 2014 [cit. 2014-04-10]. Dostupné z: https://support.google.com/drive/answer/2375123?hl=cs

Při analýze použitelnosti z hlediska právních aspektů u této služby je nutno upozornit na odstavec s názvem „Váš obsah v našich službách“[8]:

Pokud nahrajete, odešlete, uložíte nebo přijmete obsah do nebo prostřednictvím našich služeb, poskytujete společnosti Google (a subjektům, se kterými společnost Google spolupracuje) celosvětově platnou licenci k užití, hostování, uchovávání, reprodukování, upravení, vytvoření odvozených děl (například děl, jež jsou výsledkem překladu, přizpůsobení/adaptací či úprav provedených za účelem jeho lepšího fungování v rámci našich služeb), komunikaci, publikování, provozování a zobrazování na veřejnosti a distribuci takového obsahu Práva, která touto licencí udělujete jsou užita za účelem provozování, propagace a vylepšování stávajících služeb a vývoj nových služeb. Práva, která touto licencí udělujete jsou užita za účelem provozování, propagace a vylepšování stávajících služeb a vývoj nových služeb. Licence přetrvává i poté, co přestanete naše služby používat[8]

2.3. OneDrive

Službu OneDrive datujeme od roku 2007[9], tehdy se ještě jmenovala SkyDrive a přišla s ní na trh společnost Microsoft, u které byla členem rodiny Windows Live Essentials.

K přejmenování služby SkyDrive na službu OneDrive došlo v průběhu psaní této bakalářské práce, kdy společnost Microsoft prohrála soudní spor s televizní společností British Sky Broadcasting Group o název "Sky". Televizní stanice tento název používá u názvů svých televizních stanic a Microsoft u svého cloud computingu. Britský soud tedy rozhodl, že Microsoft porušuje obchodní známku

[8] Smluvní podmínky společnosti Google. Google [online]. 2014-4-14 [cit.2014-04-20]. Dostupné z: http://www.google.com/policies/terms/
[9] OneDrive. Wikipedia [online]. 2014 [cit. 2014-04-20]. Dostupné z: http://en.wikipedia.org/wiki/OneDrive

vlastněnou britskou televizní společností "BSkyB"[10]. Tato změna je pro společnost Microsoft nemalým zásahem, protože je to jedna z klíčových služeb a je integrována jak do Windows 8, Windows Phone 8, tak do mnoha dalších služeb a produktů této společnosti.

Společně se změnou názvu přišla i inovace dosud u OneDrive nepoužitá, je jí možnost navýšit svou schránku o několik stovek MB až jednotek GB. Například "pozváním přítele", kdy si někdo založí účet prostřednictvím vašeho linku. V tu chvíli dostanete 500MB jako odměnu, maximálně lze pozvat až 10 přátel, což je 5GB. Další možností je zprovoznit si synchronizaci fotek z mobilního zařízení, které je v současné době podporováno na všech mobilních platformách (iOS, Windows Phone či Android), tím si přilepšíme o další 3GB. Celkově si tedy můžeme navýšit schránku až o 8GB[11].

Přihlášení je podmíněno registrací u společnosti Microsoft, tudíž potřebujeme Windows Live ID, kdy registrace probíhá na stránce http://www.onedrive.com. Produkt OneDrive určitě nenabízí tak jednoduché rozhraní uživatele pro přístup na cloud jako jeho někteří konkurenti. Nicméně je nutno podotknout, že pro uživatele, kteří jsou zvyklí pracovat v prostředí Microsoft Windows, je toto prostředí velmi podobné a ovládání je velmi intuitivní. Po registraci a přihlášení na webovou stránku cloudu máme možnost nainstalování agenta pro synchronizaci dat se zařízením. Vzhledem k ukončení podpory systému Windows XP, jsou stávající agenti v tomto prostředí ještě plně funkční, avšak nově je již do OS Windows XP nenainstalujeme. Vytvořenou složku lze samozřejmě umístit skoro kamkoliv na pevném disku, avšak Temp je vždy umístěn automaticky v kořenovém adresáři C:\OneDriveTemp\. Velkou výhodou je implementace Word, Excel, PowerPoint a OneNote Online, nabízející nám možnost psaní nových či editování stávajících souborů. Samozřejmostí je také propojení se službou Lidé, outlook.com a kalendář. Pokud

[10] Microsoft Officially Rebrands SkyDrive To OneDrive. Techcrunch [online]. 2014-02-19 [cit. 2014-04-01]. Dostupné z: http://techcrunch.com/2014/02/19/microsoft-officially-rebrands-skydrive-to-onedrive/

[11] Správa úložiště. OneDrive [online]. 2014 [cit. 2014-04-15]. Dostupné z: https://onedrive.live.com/Options/ManageStorage?ru=https%3a%2f%2fonedrive.live.com%2f%3fgologin%3d1%26mkt%3dcs-CZ

máme v zařízení nainstalován produkt Skype, po přihlášení do webového rozhraní úložiště se nám tento promítne do webové stránky.

Tabulka 3 Cena prostoru u služby OneDrive[12]

Velikost	5GB	50GB	100GB	200GB
Cena/měsíc	Zdarma	$4,49	$7,49	$11,49

Vzhledem k propracovanosti a řešení služby lze vytknout maximální velikost uloženého souboru, 100MB[13] je v dnešní době pro mnohé opravdu málo. Nemožnost integrace agenta pro již nepodporovaný operační systém Windows XP, kdy tuto možnost zakázali neoficiálně již zhruba měsíc před ukončením oficiální podpory.

2.4. Porovnání

Všechny jmenované služby jsou velmi propracované, a co do funkcionality jim nelze prakticky nic vytknout. Ve skutečnosti jsme přišli na to, že jsme limitovaní použitelností z hlediska právních aspektů. Dropbox lze doporučit tam, kde nám nezáleží na tom, jestli jednoho dne, ať s upozorněním, či bez něho o schránku bez náhrady přijdeme. Google Drive lze doporučit pro uživatele, kteří zde nebudou nahrávat jakákoliv citlivá data, u kterých nechtějí, aby byla publikována. OneDrive lze pak použít kdekoliv tam, kde nám nebude vadit značné omezení na velikost největšího uloženého souboru. Cenové porovnání můžeme provést např. na modelové situaci o velikosti 100GB, kdy je jasně nejlevnější služba Google Drive.

Tabulka 4 Modelové porovnání jmenovaných služeb

	Dropbox	**Google Drive**	**OneDrive**
Velikost	100GB	100GB	100GB
Cena/měsíc	$9.99	$1,99	$7,49

[12] Upgrade options. OneDrive [online]. 2014 [cit. 2014-04-03]. Dostupné z: https://onedrive.live.com/Options/Upgrade?ru=https%3a%2f%2fonedrive.live.com%2f
[13] OneDrive. Wikipedia [online]. 2014 [cit. 2014-04-20]. Dostupné z: http://en.wikipedia.org/wiki/OneDrive

3. Offline files

Offline files je jedna z technologií, kterou nabízí SMB redirector na Windows operačních systémech. Offline files zajišťují lokální read/write/execute kešování sdílených souborů ze SMB souborových serverů.

3.1. Řešené operační systémy Windows

Práce se zabývá operačními systémy Windows rodiny Windows NT. Jedná se tedy Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012 a Windows Server 2012 R2. Pokud není v textu uvedeno jinak, daná technologická vlastnost se vyskytuje ve všech zmíněných systémech.

Pro úplnost je vhodné ještě uvést tabulku skutečných čísel verzí jádra (kernel) daných operačních systémů, protože dokumentace se mnohdy zmiňují přímo o těchto vnitřních číslech verzí, namísto obchodních názvů operačních systémů. V tabulce jsou současně uvedena čísla verzí protokolu SMB (Server Message Block), které jsou součástí daného operačním systému, což bude detailněji diskutováno dále.

Tabulka 5 Skutečná čísla verzí jader daných OS[14]

Obchodní název operačního systému	Číslo verze software jádra	Verze SMB protokolu	TCP transport	SMB offline files
Windows NT	4.0	1.0	139	ne
Windows 2000	5.0	1.0	445, 139	ne
Windows XP	5.1	1.0	445, 139	ano
Windows Server 2003 a Windows XP 64-bit	5.2	1.0	445, 139	ano
Windows Vista	6.0	1.0, 2.0	445, 139	ano
Windows Server 2008	6.0	1.0, 2.0	445, 139	ano
Windows 7	6.1	1.0, 2.0, 2.1	445, 139	ano
Windows Server 2008 R2	6.1	1.0, 2.0, 2.1	445, 139	ano
Windows 8	6.2	1.0, 2.0, 2.1, 3.0	445, 139	ano
Windows Server 2012	6.2	1.0, 2.0, 2.1, 3.0	445, 139	ano
Windows 8.1	6.3	1.0, 2.0, 2.1, 3.0	445, 139	ano
Windows Server 2012 R2	6.3	1.0, 2.0, 2.1, 3.0	445, 139	ano

3.2. Technologie sdílených souborů v operačních systémech Windows

Ve Windows je k dispozici několik protokolů sdílených souborů, jako je SMB (Server Message Block), WebDAV (Web Distributed Authoring and Versioning), nebo TSClient (Terminal Services Client File Access). Technologie sdílených souborů je rozšiřitelná, je tedy potřeba uvědomit si nejprve její strukturu a funkci.

Pod pojmem technologie sdílených souborů se rozumí obecně síťová technologie klient-server, která umožňuje klientské aplikaci přistupovat na soubory umístěné na lokálních datových úložištích serverové strany. Serverová aplikace tak „sdílí“ lokální soubory do sítě pro klientské aplikace. Datovými úložišti serverové strany může být obecně cokoliv, typicky například lokální diskový souborový systém

[14] Timeline of Microsoft Windows. Wikipedia [online]. 2014-02-18 [cit. 2014-04-10]. Dostupné z: http://en.wikipedia.org/wiki/Timeline_of_Microsoft_Windows

(typicky NTFS), nebo databázový server a jeho databázové soubory (jako je například SQL Server v případě webového serveru SharePoint).

Serverová aplikace může běžet buď na jiném počítači v síti, nebo i lokálně na stejném počítači se software klienta. V obou případech by měl být přístup pro uživatele klientské aplikace transparentní tak, aby si uživatel nemusel uvědomovat, kde v síti a na kterém počítači běží aplikace serveru, a kde jsou tedy soubory fyzicky uloženy.

Technicky se dnes bude jednat vždy o ustavení TCP/IPv4 nebo TCP/IPv6 spojení mezi klientskou aplikací a aplikací serveru. Serverová aplikace k tomu tedy tak zvaně „poslouchá“ na nějakém TCP portu. Klientská aplikace se na takový serverový TCP port připojuje ze svého dočasného (tzv. ephemeral TCP portu).

V jádře (kernel) Windows existuje obecná a rozšiřitelná architektura pro implementaci klientské strany přístupu ke sdíleným souborům. Tato architektura se snaží umožnit uživatelským aplikacím jednotnou formu přístupu k souborům, ať už na lokálních diskových souborových systémech (jako je NTFS, nebo FAT), nebo přes síť přes nějaký ze síťových protokolů sdílených souborů.

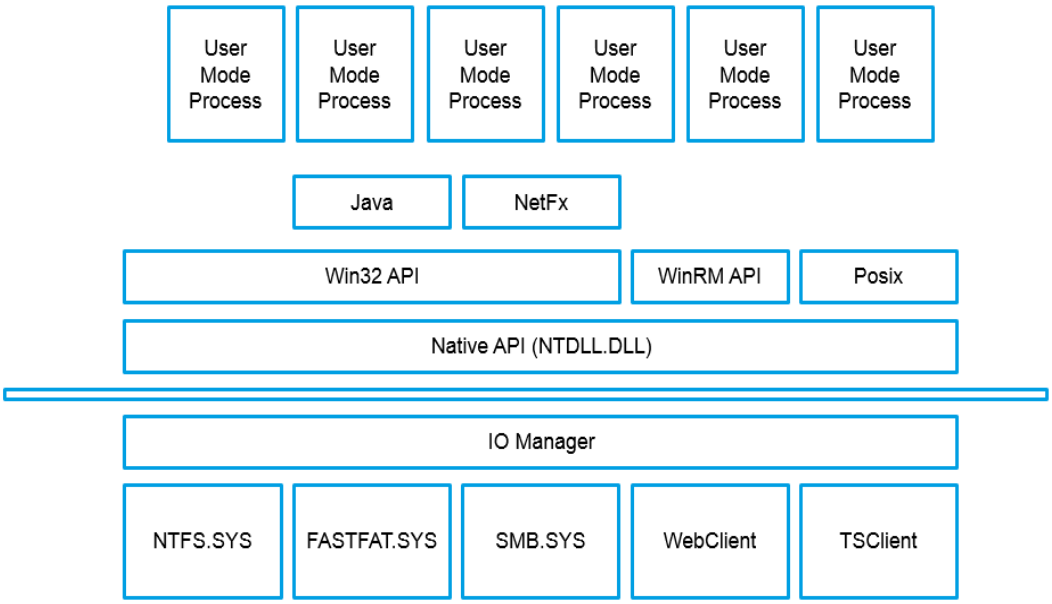
Pro aplikace používající Win32 API, NativeAPI, nebo WinRM API a Posix je přístup a práce se soubory stejná, bez ohledu na jejich fyzické umístění nebo protokol přístupu.

Toho se dosahuje pomocí klientské knihovny jádra, nazývané redirector. Klientská knihovna jádra se realizuje jako tzv. ovladač jádra, tedy v podstatě DLL knihovna s příponou SYS, která se načítá do jádra operačního systému místo, aby se jako DLL knihovna načítala do paměti konkrétního procesu běžícího v uživatelském režimu. Pro každý protokol sdílených souborů je možno vytvořit separátní takový redirector, který bude obsluhovat požadavky z klientských aplikací běžících v uživatelském režimu.

Klientské aplikace v podstatě volají nepřímo jen souborové funkce nativního API jádra operačního systému, jako je například NtCreateFile, NtOpenFile, NtReadFile, NtWriteFile apod., které tyto požadavky předávají přes další rozhraní IO

Manageru (komponenta jádra) do konkrétního redirectoru pro daný soubor. Vnitřní struktura a funkce komponenty jádra zvané IO Manager není pro nás zde důležitá.

Z pohledu klientské aplikace, která chce pracovat se souborem, se jedná čistě o zavolání nějaké své API funkce (například Win32 API, .NET Framework, Java, WinRM apod.) jejíž kód transparentně a nepřímo zavolá zmíněné funkce IO Manageru (například právě NtCreateFile) a IO Manager už se postará o přesměrování daného požadavku buď na lokální diskový souborový systém (jako je NTFS), nebo právě na nějaký síťový souborový systém (jako je právě SMB). Architektura je názorně vyobrazena na následujícím obrázku.



Obrázek 1 Native API Převzat a zjednodušen z knihy Windows Internals, Mark Russinovich[15]

Tato architektura identifikuje soubory v podstatě jednotnou formou adresy (cestou k souboru), ať leží lokálně, nebo na síti. Cesta k souborům umístěným lokálně začíná běžně písmenem oddílu, následovaným dvojtečkou a zpětným lomítkem. Cesta ke sdíleným souborům začíná obvykle buď dvěma zpětnými

[15] RUSSINOVICH, Mark E, David A SOLOMON a Alex IONESCU. Windows internals. 6th ed. Redmond: Microsoft Press, 2012, xxii, 726 s. ISBN 978-0-7356-4873-9.

lomítky, nebo například prefixem http:// v případě WebDAV sdílených souborů. Následující tabulka ukazuje příklady některých cest k souborům.

Tabulka 6 Příklady cest k souborům

Příklad cesty k souboru	Technologie
C:\Nabidky\zakaznik0015943-nabidka1.docx	NTFS lokální diskové soubory na pevném disku
F:\Fotky\dovolena0035.jpg	CDFS nebo UDF lokální diskové soubory na CD
G:\Zalohy\BP-Kubes_tabulky.xlsx	FAT lokální diskové soubory na přenosném USB flash disku
\\fileserver\Dokumentace\BP-Kubes.pdf	SMB sdílený soubor z počítače fileserver, ke kterému se přistupuje pomocí jeho UNC cesty
\\fileserver.ad.jcu.cz\Dokumentace\BP-Kubes.pdf	Stejný SMB sdílený soubor z počítače fileserver, na který se přistupuje pomocí UNC zadané za pomoci FQDN počítače serveru
\\fs.ad.jcu.cz\Dokumentace\BP-Kubes.pdf	SMB sdílený soubor z počítače fileserver, na který se přistupuje přes CNAME DNS alias fs při použití jeho kompletního FQDN
\\160.217.6.68\Dokumentace\BP-Kubes.pdf	Stejný SMB sdílený soubor z počítače fileserver, na který se přistupuje přes IP adresu počítače serveru
http://intranet/excel/tabulky/kubes-tab1.docx	Sdílený soubor umístění v síti na serveru intranet ve webovém serveru SharePoint, na který se přistupuje pomocí WebDAV protokolu přes HTTP
https://intranet.jcu.cz/excel/tabulky/kubes-tab1.docx	Stejný WebDAV soubor s přístupem přes TLS zašifrované HTTPS za použití jiného DNS aliasu pro IP adresu serveru

\\intranet\davWWWroot\excel/tabulky/kubes-tab1.docx	Stejný WebDAV soubor s přístupem přes protokol HTTP, ovšem za použití více kompatibilní tradiční UNC cesty začínající dvěma zpětnými lomítky
\\tsclient\c\Dokumenty\vykres1.dwr	Soubor na disku C:\ na počítači Terminal Services klienta (novější Remote Desktop klienta), ke kterému se přistupuje z terminálové relace z terminal serveru (novější remote desktop serveru)

Poznámka - cesta k souboru začínající dvěma zpětnými lomítky se nazývá UNC cesta (Unified Naming Convention). Jak bylo vidět v tabulce, například WebDAV umožňuje přístup jak pomocí běžného URL, tak i pomocí UNC cesty, která je vhodnější pro mnohé zastaralejší, nekompatibilní aplikace, které nejsou schopny zpracovávat URL při přístupu k souborům.

Jak by mělo být z předchozí tabulky a jejích příkladů zřetelné, jádro Windows, přesněji jeho komponenta IO Manager, umí přijímat různě zadané cesty k souborům, jak lokálním, tak síťovým, a požadavky na tyto soubory provede standardní a transparentní metodou a poskytuje tak aplikacím běžícím v uživatelském režimu ve všech případech srovnatelnou službu. Jádro tak odstiňuje aplikace od fyzické podstaty a přenosových protokolů u souborů, se kterými pracují.

Z důvodu toho, že uživatelé jsou mnohdy zvyklí pracovat se soubory za pomoci písmene disku, jádro operačního systému umožňuje tzv. mapovat písmena disků na síťové souborové cesty. Vytvoří se tak vlastně alias ve formě písmene disku, který se ve skutečnosti, ještě před tím, než se požadavek zašle do konkrétního redirectoru, přeloží na skutečnou UNC, nebo jinou síťovou cestu, které daný redirector rozumí.

Znamená to, že uživatel může pracovat se soubory například přes písmeno H:\, zatímco toto se, lokálně na jeho stanici, překládá na skutečnou UNC cestu \\serverREK\home\REK\.

Jádro Windows umí mapovat libovolné síťové cesty podporované nějakým redirectorem na písmena disku. Je tedy možné mapovat na písmeno disku jak UNC cestu začínající dvěma zpětnými lomítky, tak i HTTP URL začínající prefixem http:// nebo https:// podle příkladů v předchozí tabulce.

Z pohledu redirectoru samotného se ovšem vždy jedná přesně pouze o síťovou cestu, které on sám rozumí. Redirector sám nemá ponětí o diskovém mapování.

Mapovaný disk je také dobrou metodou, jak zajistit alespoň částečnou kompatibilitu se starými MS-DOS programy, které síťovým cestám, jako je UNC, nebo URL dosud vůbec nerozumí. Ani dnes není moc běžné, aby ani programy určené pro Windows 7, nebo Windows 8 rozuměly například URL (tedy HTTP) cestám k souborům, byť tuto technologii Windows nabízí již od verze Windows XP (zmiňovaný WebClient). Mapovaný disk pak umožňuje, aby aniž by to program sám věděl, používal pro sebe srozumitelnou diskovou cestu simulovaného lokálního disku a nechal jeho síťovou podstatu na jádře operačního systému, které ji pro redirector samo překládá.

3.3. Protokoly SMB a jejich verze ve Windows

Ve Windows je k dispozici server i klient (tedy právě klientský redirector) sdílených souborů na protokolu SMB (Server Message Block), což historicky vychází z protokolu Lan Manager, který Microsoft implementoval pro IBM OS2. Protokol SMB je občas nazýván také CIFS (Common Internet File System), což je název pro totéž a je možné je zaměňovat. V textu budeme ale okazovat pomocí častějšího SMB.

Pro Linux existuje implementace téhož protokolu, jak jeho server, tak i klientské části, jako software zvaný Samba. Tento software není nijak podporován ze strany Microsoftu a není možné ho považovat za plně kompatibilní. Tento materiál se

Samba implementací tedy nebude vůbec zabývat. To znamená, nediskutujeme ani MS klienta versus Samba Server, ani opačně, protože nemůžeme spoléhat na kompatibilitu.

SMB protokol pracuje od Windows 2000 primárně nad TCP 445. Pokud spojení na tomto portu není k dispozici, je buď blokováno nějakým firewall v cestě, nebo je klient, nebo server na verzi Windows NT 4.0 a starší, spojení se navazuje pomocí NetBIOS Session Service (v případě přenosu NetBIOS přes TCP – tzv. NetBIOS over TCP - na portu TCP 139).

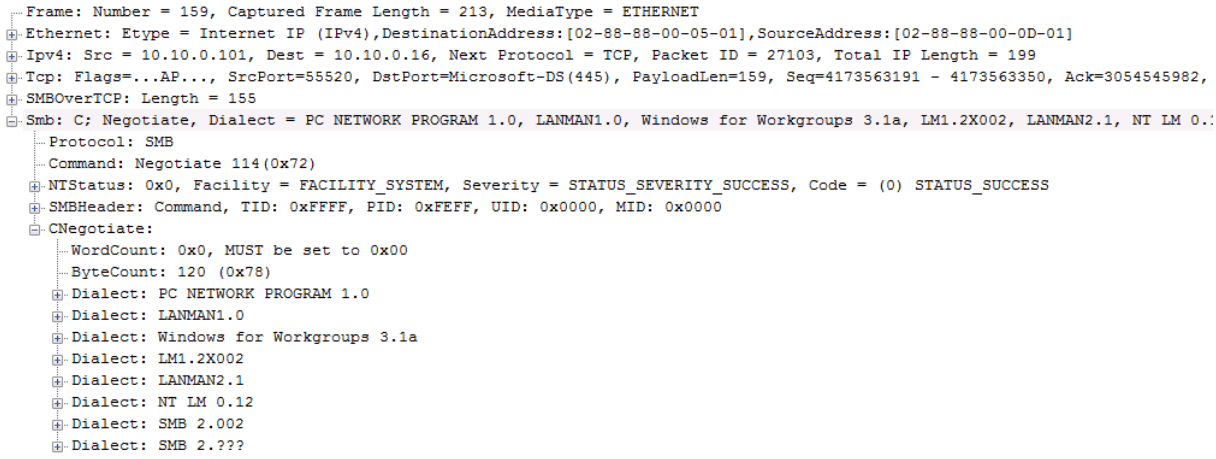
SMB protokol prošel za posledních 20 let několika úpravami, konkrétně je k dispozici ve verzích 1.0, 2.0, 2.1 a 3.0. Verze 3.0 byla původně číslována pouze jako 2.2, ale vzhledem k mnoha výkonovým vylepšením, která přišla ve Windows Server 2012 a Windows 8, byl přečíslován na verzi 3.0.

Novější verze byly hlavně výkonově vylepšeny, bylo zmenšeno množství jednotlivých paketových výměn (round-trip), které jsou nutné k domluvě a přenosu parametrů přenosu a metadat jednotlivých souborů a adresářů a jejich zabezpečení. Například verze 3.0 nabízí dokonce transparentní fail-over, tedy v případě klastrovaného souborového SMB serveru se klient umí bez výpadku připojit na jiný člen clusteru.

Microsoft prohlašuje všechny tyto čtyři verze za vzájemně kompatibilní ve vztahu klient-server. To znamená, že klient se SMB 1.0 se musí být schopen bez problémů připojit na SMB server, který implementuje i novější verze protokolu. A naopak, i SMB klient, který implementuje verzi 3.0, umí i všechny starší verze protokolu a umí se tak připojit i na SMB Server, který umí pouze verzi 1.0. K tomu je v úvodní SMB paketové výměně zavedena metoda domluvy verze protokolu (version negotiation).

Následující obrázek ukazuje screen-shot z programu Microsoft Network Monitor, který zachycuje první SMB paket poslaný ze SMB klienta na SMB server – tzv. CNegotiate (C jako client). V paketu je vidět seznam klientem podporovaných dialektů. Z tohoto seznamu si SMB server vybere nejnovější verzi protokolu, kterou

sám podporuje. SMB server potvrdí tuto verzi klientovi v paketu RNegotiate (R jako repsonse).



Obrázek 2 První paket ze SMB klienta na SMB server

Všechny verze SMB serveru nabízí z našeho pohledu tyto služby podstatné pro funkci offline files:

a) create/read/write/execute/delete přístup k souborům na SMB serveru s libovolným lokálním souborovým systémem (NTFS, FAT, apod.)
b) create/list/delete přístup k adresářům na SMB serveru s libovolným lokálním souborovým systémem (NTFS, FAT, apod.)
c) čtení a změna NTFS metadat souborů a adresářů na SMB serverech, zvláště časových razítek změny a vytvoření souboru, nebo adresáře
d) čtení a změna NTFS zabezpečení souborů a adresářů na SMB serverech
e) zamykání souborů a adresářů na vzdálených SMB serverech pro sdílený z více klientů i výhradní přístup z jediného klienta a jeho jediného aplikačního procesu
    a. ve verzi SMB 1.0 zámek souboru, nebo adresáře trvá pouze maximálně po dobu trvajícího TCP spojení mezi SMB klientem a SMB serverem
    b. od verze SMB 2.0, je zámek souboru držen, na straně serveru i klienta, ještě dalších 20 sekund i po skončení TCP spojení a je možno ho navázat dalším TCP spojením mezi stejnými operačními systému

SMB klienta a SMB serveru pod stejnou uživatelskou identitou. Tím se dosahuje lepší návaznosti spojení při cestování uživatelů s počítačem (notebook, tablet), například na WiFi, nebo mobilním spojení

c. v případě SMB verze 3.0 se zámek zachová i v případě, že dochází k transparentnímu fail-over mezi členy SMB serverového klastru, který implementuje sdílené adresáře na technologii cluster shared volume (CSV).

Zvláště zámky souborů a jejich chování zvláště na verzích SMB 2.0 a novějších, jsou velmi podstatnou součástí funkce SMB protokolu. Umožňují klientským aplikacím, aby si otevřely soubory a adresáře k výhradnímu přístupu, a výhradní přístup nemusí být ztracen ani při občasných krátkých výpadcích TCP konektivity.

Z předchozího plyne, že na protokolové úrovni jsou různé verze SMB klientů a SMB serverů kompatibilní. Z pohledu technologie offline files je tedy jejich verzování nepodstatné.

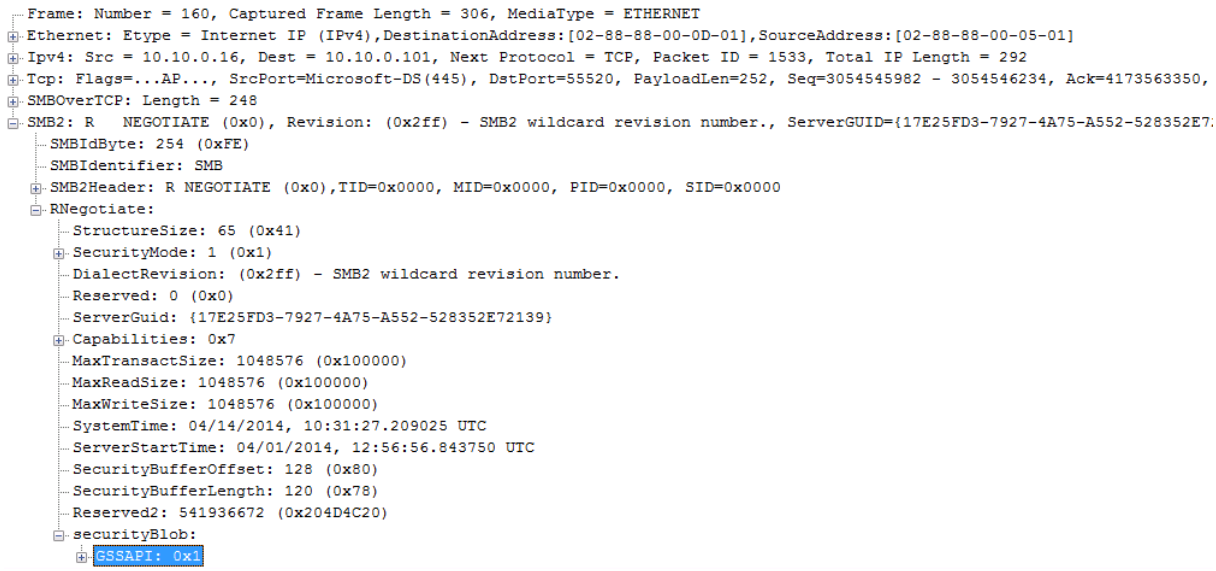
Za druhé je vhodné si uvědomit následující. Pokud má SMB klient zámek souboru, nebo adresáře na SMB serveru, a pokud současně ztratí TCP spojení se svým SMB serverem, je nutno počítat obecně s tím, že během několika málo sekund bude soubor na serverové straně odemknut. A bude následně moci docházet k modifikacím souborů, nebo k jejich zamykání z jiných SMB klientů a aplikací.

3.4. Ověřování uživatelů vůči SMB serverům

SMB protokol implementuje ověřování uživatelských účtů pro každé ustavované TCP spojení pomocí obecného GSS-API protokolu. Ověření je jednorázové, vždy pro nově vznikající SMB spojení se SMB serverem. GSS-API nabízí generickou domluvu (negotiation) ověřovacího (authentication) protokolu.

Podobně, jako SMB klient sám o sobě nabízí SMB serveru verze SMB protokolu, které sám podporuje. V případě GSS-API začíná s nabídkou možných

ověřovacích protokolů strana SMB serveru (přesněji GSS-API server), která nabízí SMB klientovi (přesněji GSS-API klientovi) autentizační metody, které sama podporuje. Nabídka GSS-API ověřovacích metod je součástí druhého SMB paketu, prvního ve směru ze SMB serveru na SMB klienta, tedy již zmíněného RNegotiate. Viz. následující screen-shot získaný z programu Microsoft Network Monitor, kterým je možno odchytávat pakety putující po síťovém rozhraní.



Obrázek 3 GSSAPI

Windows implementují v GSS-API buď NTLM, nebo Kerberos ověření uživatelského účtu, s tím, že Kerberos je primární preferovaná metoda. Pokud Kerberos nelze použít, sklouzne se (fall-back) na starší, a méně bezpečné, NTLM.

Kerberos nabízí moderní, otevřený ověřovací standard, který provádí vzájemné ověření (mutual authentication) uživatele, jeho řadiče domény i cílového síťového serveru nebo služby. Provádí pře-klíčování (rekeying) po určitém čase a má ochranu proti reply útokům (přeposílka). Šifruje za určitých podmínek pomocí AES. Naopak NTLM nenabízí vzájemné ověření a má jen omezenou ochranu proti reply útokům. NTLM šifruje pouze pomocí HMAC-MD5 a od roku cca 1998 se dále nijak nevyvíjí.

GSS-API strana serveru nabízí klientovi Kerberos ověřování jen v případě, že počítač SMB serveru je členem Active Directory domény. V případě, že počítač SMB serveru není členem Active Directory domény, jediná možnost je použít NTLM authentication. NTLM ověřovací protokol je ovšem nabízen v obou případech.

Klient GSS-API si může vybrat Kerberos ověření pouze, pokud i počítač SMB klienta je členem nějaké Active Directory domény. Nemusí jít nutně o stejnou Active Directory domény, jejímž členem je počítač SMB serveru. Nutně se ovšem vyžadují následující podmínky pro to, aby Kerberos ověření vůbec mohlo proběhnout a bylo úspěšné:

a) počítač SMB serveru je členem domény Active Directory, ve které funguje Kerberos Key Distribution Center (KDC)
b) počítač klienta SMB musí být členem domény Active Directory, ve které také funguje KDC
c) k přístupu na SMB server se musí použít uživatelský účet, který je definován v nějaké Active Directory doméně, ve které také funguje KDC
d) pokud jsou uživatelský účet použití ze SMB klienta a počítač SMB serveru v jiných Active Directory doménách, musí mezi nimi existovat přímý, alespoň jednosměrný, forest trust – odchozí ve směru k uživatelské doméně, tedy doména počítače SMB serveru musí být trusting (neboli resource domain). Pouze forest trust nabízí Kerberos ověření
e) pokud je forest trust nastaven jako selektivní (selective trust), musí být danému uživateli povoleno ověřování vůči účtu daného počítače SMB serveru (pomocí Allowed to Authenticate rozšířeného Active Directory oprávnění)
f) oba počítače a všechny řadiče Active Directory domény (domain controller) musí mít synchronizovaný čas, s rozptylem nejhůře +/- 5 minut
g) pro přístup na počítač SMB serveru se musí v UNC cestě použít, na straně SMB klienta, pouze jméno – buď krátké jméno, nebo DNS FQDN (plně kvalifikované DNS jméno – fully qualified DNS name). Pokud se použije

IPv4, nebo IPv6 adresa v UNC cestě, Kerberso není možný a sklouzne se na NTLM

h) pokud se v UNC cestě na straně SMB klienta použije místo názvu SMB serveru jeho DNS alias (například CNAME, nebo jiný A záznam), je nutné, aby pro tento alias bylo správně nadefinované service principal name (SPN). Service principal name je řetězec ve formě cifs/alias.fqdn, který musí být asociován s účtem počítače SMB serveru v jeho Active Directory doméně. Asociace SPN s účtem se provádí pomocí atributu účtu servicePrincipalName. Bez koretního SPN záznamu na účtu počítače SMB serveru není Kerberos možný
i) při přístupu přes trust je nutné, aby se v UNC cestě zadané na straně SMB klienta použilo plně kvalifikované DNS jméno počítače SMB serveru (FQDN)

Pokud tyto podmínky nejsou splněny, klient sklouzne na ověření pomocí NTLM. A to typicky v těchto běžných situacích

a) k přístupu na SMB server se použije lokální účet definovaný na počítači SMB serveru
b) k přístupu se na straně SMB klienta, v zadané UNC cestě, použije IPv4, nebo IPv6 adresa, namísto jména počítače SMB serveru
c) k přístupu se na straně SMB klienta, v zadané UNC cestě, použije namísto skutečného jména počítače SMB serveru jeho jmenný DNS alias (ve formě CNAME, nebo dalšího A záznamu) a přitom není správně nakonfigurováno Kerberos SPN (service principal name).

Obě metody, jak Kerberos, tak i NTLM, jsou úplně transparentní pro implementaci SMB klienta i SMB server. Je to tak, protože o ověřování uživatelů a vyhodnocení jejich identit se stará GSS-API a potažmo bezpečnostní subsystém počítače SMB klienta i SMB serveru. Bezpečnostní subsystém je implementován v systémovém, user-mode procesu LSASS.exe (local security sub-system).

SMB protokol všech verzí pouze využívá GSS-API k tomu, aby přenášel generické ověřovací informace pro libovolný z obou protokolů, ať už Kerberos, nebo

NTLM. Ve skutečnosti tak funguje pouze jako přenašeč těchto ověřovacích informací mezi LSASS na straně SMB klienta a LSASS na straně SMB serveru, aniž by vůbec řešil obsah těchto autentizačních dat.

To, co SMB server potřebuje z GSS-API (a potažmo LSASS) autentizační výměny získat, je pouze paměťová struktura nazvaná access token. Access token obsahuje údaje o identitě přistupujícího ověřeného uživatele, tedy jeho login, jméno domény, SID (security ID) a seznam SIDů všech doménových skupiny a skupin lokálních na počítači SMB serveru, ve kterých byl uživatel v okamžiku ověření členem.

Teprve tuto paměťovou strukturu (access token) potom SMB server využívá k ověření přístupových oprávnění daného uživatele na souborové prostředky lokálního počítače SMB serveru. Umožňuje mu to ověřit, zda a jaký má mít daný uživatel na daném TCP SMB spojení konkrétně přístupy k souborům a adresářům, které požaduje.

Zabezpečení přístupu je striktně vymáháno na straně SMB serveru. Ve směru k SMB klientovi neputují data, ke kterým by daný uživatel neměl přístup současně i na lokálním souborovém systému SMB serveru.

3.5. Automatické přihlašování na síťové prostředky, neboli single-sign-on (SSO)

Jak bylo řečeno, prokazování uživatelské identity a jeho ověřování a přijímání, realizuje bezpečnostní subsystém (LSASS) počítačů SMB klienta a SMB serveru. Toto ověřování samo o sobě není nijak závislé na použité verzi SMB protokolu a implementace SMB klienta i SMB serveru se jím vůbec nezajímá, kromě faktu, že musí používat určité implementační API protokolu GSS-API.

LSASS se primárně snaží o automatické přihlašování a tedy automatické poskytování ověřené identity uživatele (single-sign-on, neboli SSO), přihlášeného a pracujícího na počítači SMB klienta do sítě. LSASS primárně a automaticky používá zašifrované přihlašovací údaje, které mu uživatel svěřil při lokálním přihlášení na počítači SMB klienta.

LSASS na straně SMB klienta je ochoten odeslat svěřené přihlašovací údaje, v zašifrované formě, na síťové servery. Dělá to automaticky, na žádost GSS-API ze SMB serveru.

V podstatě to funguje tak, že uživatel zadá své přihlašovací údaje pouze jednou, při přístupu na svoji pracovní stanici (tedy buď heslo, nebo čipovou kartu). Takové údaje se nazývají výchozí (default credentials). Od toho okamžiku jsou přihlašovací údaje i Kerberos tikety uloženy v chráněné systémové paměti LSASS procesu. Kdykoliv jsou potřeba, GSS-API a protokoly Kerberos a NTLM si je mohou vyzvednout a transparentně použít proti libovolným síťovým prostředkům. A to bez žádání uživatele o interakci.

Zde je dobré zopakovat, že Kerberos je použije bezpečně, pouze proti vzájemně ověřeným síťovým serverům, na rozdíl od NTLM, které je ochotné je odeslat na jakoukoliv síťovou službu, protože neumí provádět vzájemné ověření (mutual authantication).

Uživatel také může do paměti LSASSu, ve svém kontextu, v průběhu své práce a svého přihlášení, přidat další přihlašovací údaje – tzv. fresh credentials. Například pokud nechce, aby se jeho výchozí přihlašovací údaje použily vůči nějakému SMB serveru, ale přeje si, aby se použily jiné. K tomu je možné využít například známý příkaz NET USE, nebo RUNAS.

Takové doplněné přihlašovací údaje jsou vázané na název (host name, neboli host header) vzdálené služby. Takže LSASS je uchovává v paměti po dobu uživatelova přihlášení, ale vydá je jen v případě, že si o ně řekne právě daná síťová služba s daným jménem. Tedy typicky, podle jména, nebo IP adresy, použité v UNC cestě k síťovému souborovému prostředku.

Zde je vhodné upozornit, že LSASS rozlišuje cílové služby přesně podle jejich jména (host header, neboli host name). Z pohledu LSASS jsou tedy například jména fileserver a fileserver.ad.jcu.cz rozdílné a mohou používat různé přihlašovací údaje. Stejně tak se LSASS nezabývá IP adresou síťového prostředku. To znamená, že například jména fileserver, fileserver.ad.jcu.cz i 160.217.5.3 jsou různá jména a

mohou používat různé přihlašovací údaje, bez ohledu na to, že se je možná jedná o službu běžící na stejném síťovém počítači.

3.6. Technologie SMB na Jihočeské univerzitě v Českých Budějovicích

JU implementuje jedinou Active Directory doménu s DNS názvem ad.jcu.cz a NetBIOS názvem JCU. V doméně jsou připojeny jak počítače uživatelů, fungující jako SMB klienti, tak i počítače SMB serverů. Všichni uživatelé pracují po přihlášení na stanicích pod svým Active Directory doménovým uživatelským účtem. K němu se přihlašují buď za pomoci uživatelského loginu a hesla, nebo za pomoci čipové karty a znalosti jejího PIN.

V obou případech jim LSASS ukládá v paměti potřebné Kerberos ověřovací tikety, případně NTLM heš hesla. Tyto údaje tak může využít k poskytování single-sign-on vůči SMB serverům.

V síti JU se vyskytují klientské počítače s operačními systémy Windows XP, Windows Vista, Windows 7 a novějšími. Servery SMB jsou vybudovány na Windows 2008 R2 a Windows 2012. Znamená to, že se v síti používá protokol SMB verze 1.0 (z Windows XP) i libovolný novější (z novějších systémů).

Doména Active Directory ad.jcu.cz pracuje na úrovni funkčnosti domény (domain functional level – DFL) Windows 2008 R2. Díky tomu ověřovací protokol Kerberos, pokud je použit z klientského počítače s Windows Vista a novějším, vůči souborovému serveru s operačním systémem Windows 2008 a novějším, může šifrovat pomocí moderního AES.

NTLM je v síti povoleno, není zakázáno z důvodu kompatibility. Používá se minimálně, protože všechny podmínky umožňují použití protokolu Kerberos při přístupu na SMB souborové servery.

V sítí JU v prostředí souborových služeb domény ad.jcu.cz plně funguje single-sign-on (SSO) automatické přihlašování.

SMB sdílené soubory se využívají primárně ke třem účelům

a) ke stahování cestovních profilů uživatelů (roaming profiles). Uživatelské profily jsou vždy zpracovávány na stanicích pouze lokálně. Pokud je ovšem pro určitý uživatelský účet implementována metoda cestovních profilů, celý profilový adresář je synchronizovaná ze SMB serveru na lokální stanici v průběhu přihlašování. Profilový adresář je opět synchronizován zpět na SMB server v průběhu odhlašování ze stanice. Celý objem uživatelského profilu zůstává přítomen na stanici i po odhlášení uživatele. Lokální profilový adresář je umístěn na Windows XP typicky v adresáři %systemroot%\Documents and Settings\%username% a od Windows Vista v adresáři %systemroot%\Users\%username%.

   Pokud je v jednom z těchto momentů SMB server nedostupný (typicky od sítě odpojený notebook), synchronizace neproběhne a znovu se o ni stanice pokouší při dalším přihlášení, nebo odhlášení daného uživatele. Zde se nejedná o použití offline files (viz. dále). Synchronizace obsahu profilového adresáře probíhá na úrovni celých souborů, na základě jejich časových razítek poslední změny.

   UNC cesta k cestovnímu profilu každého uživatele je definována ve vlastnostech Active Directory účtu daného uživatele na záložce Profile. Jedná se o LDAP atribut profilePath.

   V případě cestovního profilu tedy uživatel vždy pracuje pouze s lokálními soubory na stanici, jejichž změny se mohou při odhlášení a přihlášení uživatele odkopírovat na souborový server. Děje se tak na pozadí a uživatel nemusí o tomto procesu v podstatě vůbec vědět.

   K souborům, které jsou součástí profilu (typicky například %temp%), uživatel tedy přistupuje obvykle buď do podadresáře v %systemroot%\Documents and Settings\%username% (na Windows XP), nebo do podadresáře v %systemroot%\Users\%username% (na Windows Vista a novějších) a nezajímá se o jeho synchronizaci na souborový server.

b) k online přístupu do domovských adresářů uživatelů. Každý uživatel má na SMB serveru k dispozici svůj vlastní soukromý prostor pro ukládání dokumentů a dalších datových souborů. K přístupu do svého domovského adresáře může uživatel využít jeho UNC cestu, pokud by ji znal. Vzhledem

k zbytečné komplikovanosti takového přístupu, se uživatelům vytváří automaticky namapovaný disk H:, který zakrývá síťovou podstatu takových souborů.

Znamená to například, že když uživatel s loginem „kubes“ přistupuje na soubor například H:\dokumentace.docx, ve skutečnosti přistupuje na SMB sdílený souboru \\serverREK\home\REK\zam\k\kubes.

Uživatelé mají jen minimální ponětí o tom, že u disku H: se jedná ve skutečnosti o „síťový disk“ a že soubory jsou principiálně dostupné pouze online. V tomto případě je vhodné využít technologii offline files (viz. dále) k tomu, aby uživatelé měli soubory dostupné i v případě výpadku konektivity na SMB server (například při odpojeném notebooku, doma nebo na služební cestě).

Mapování disku H: na síťovou SMB UNC cestu k domovskému adresáři uživatele zajišťuje opět přihlašovací proces, který tuto cestu načte z Active Directory účtu uživatele při přihlášení a mapovaný disk H: vytvoří. Cesta k domovskému adresáři i písmeno disku, které se má k mapování použít, jsou definovány na záložce Profile ve vlastnostech uživatelského účtu v Active Directory. Jedná se o LDAP atributy homeDrive a homeDirectory.

c) k online přístupu na přesměrované dokumenty a obsah plochy (tzv. folder redirection). Pro uživatele je mnohdy i namapovaný domovský disk H: poměrně složitý koncept. Většina GUI rozhraní pro ukládání a otevírání souborů průzkumníka Windows (Windows Explorer) nabízí primárně nikoliv umístění na domovský disk, ale naopak zobrazuje ve výchozím stavu obvykle buď složku Dokumenty (Documents), nebo služku Plocha (Desktop). Pokud si uživatel chce své soubory uložit do domovského adresáře, znamenalo by to pro něho jeden až dva zbytečné kliky navíc. Dokumenty a Plocha jsou jednoduše více po ruce.

   Z toho důvodu průzkumník Windows nabízí ještě další možnost zakrytí skutečné UNC síťové souborové cesty. Jedná se o možnost změnit fyzické umístění složky Dokumenty a Plocha. Ve výchozím stavu jsou ukládány do uživatelského profilu. Pomocí ručního, nebo centrálního nastavení je však možné změnit jejich umístěni na síťovou UNC cestu.

Zde se nejedná o skutečné mapování disku, ale jen o GUI znázornění v průzkumníkovi Windows. Zatímco mapovaný disk je vlastnost jádra operačního systému a jeho komponenty IO Manager, přesměrované složky se jeví jako lokální pouze v průzkumníkovi Windows. Programy však ve skutečnosti přistupují přímo do UNC cesty a musí tento její UNC formát tedy podporovat.

Přesměrované dokumenty tak fungují jako další automatické přístupy na online síťové souborové prostředky. Opět vyvstává problém s odpojením počítače od SMB serveru. V okamžiku ztráty konektivity by byly obsahy složek Dokumenty a Plocha nedostupné a ze zobrazení by zmizely.

Pro shrnutí tedy, uživatelé v Active Directory prostředí na JU využívají, aniž by o tom sami nutně věděli, ve skutečnosti tři síťové souborové SMB servery. Používají ho ke stahování a ukládání obsahů svých lokálních profilů – tedy mají cestovní profily. Jejich obsah mají trvale na svých počítačích a je tedy dostupný i při odpojení počítače od sítě. Cestovní profil tak plní jednak funkci záložní, případně se pak kopíruje na nový počítač, kde uživatel dosud nepracoval, nebo se již delší dobu nepřihlásil.

Používají však SMB síťový přístup také k práci se svými domovskými adresáři, které jsou mapované na písmeno H. Do tohoto adresáře vstupují principiálně online přes SMB spojení se SMB serverem. V případě výpadku konektivity by byl obsah dané UNC cesty domovského adresáře (a potažmo simulovaného disku H) nedostupný.

Druhý online SMB síťový přístup realizují, aniž by to tušili, když pracují s dokumenty, které se jeví, že jsou uložené ve složce Dokumenty, nebo se zobrazují na Ploše počítače. Zde se opět jedná o online SMB síťový přístup. V případě výpadku konektivity by obsahy složky Dokumenty a Plochy opět zmizely a staly se nedostupnými.

Následující tabulka shrnuje stav v prostředí Active Directory domény ad.jcu.cz. Uveden je kompletně pouze příklad ústavu REK. UNC cesty pro ostatní fakulty sledují stejnou šablonu pouze se změněnou třípísmennou zkratkou ústavu

(fakulty). V případě UNC cesty k cestovnímu profilu a UNC cesty k domovskému adresáři uživatele je cesta ještě pod-strukturována prvním písmenem loginu uživatele – uživatelé tuto UNC cestu v podstatě sami nepoužívají – jedná se o lepší přehlednost pro správce lokálního diskového souborového systému daných SMB souborových serverů.

Tabulka 7 UNC cesty

Uživatelé z fakulty	**UNC cesta k profilům**	**UNC cesta k domovskému adresáři**	**UNC cesta k přesměrovaným složkám**
FEK			
FFI			
FPE			
FPR			
FRO			
FTE			
FZE			
FZS			
KAM			
REK	\\serverREK\profiles\REK\zam\<prvnipismenologinu>\<login> \\serverREK\profiles\REK\stud\<prvnipismenologinu>\<login>	\\serverREK\home\REK\zam\<prvnipismenologinu>\<login> \\serverREK\home\REK\stud\<prvnipismenologinu>\<login>	\\serverREK\Redir\REK\<login>\Desktop \\serverREK\Redir\REK\<login>\My Documents
SZP			
UFB			

Oba dva případy online přístupu a výpadku jejich konektivity řeší technologie offline file.

3.7. Technologie offline files obecně

Pro zopakování, SMB redirector je klient SMB sdílených souborů fungující jako knihovna v jádře (kernel) operačního systému Windows. Veškeré přístupy na

UNC síťové SMB cesty jsou zasílány do tohoto redirectoru. Jádro systému umožňuje sice namapovat nad UNC cestu písmeno disku, ale z pohledu redirectoru se jedná vždy už pouze o konkrétní UNC cestu a její podcesty.

SMB redirector umožňuje pracovat s obsahem vzdálených souborů, adresářů a s metadaty vzdálených souborových systémů online. V případě, že ještě nemá ustaveno TCP spojení se SMB serverem, pokusí se takové vytvořit. Ve vytvořeném TCP SMB spojení proběhne následně i ověření uživatele pomocí GSS-API, primárně tedy Kerberos, případně fall-back na NTLM.

SMB redirector implementuje navíc lokální keš SMB sdílených souborů. Jeho keš je ve výchozím stavu vypnutá. Pokud ji chce uživatel využívat, musí si ji buď sám zapnout, nebo ji může správce počítače zapnout centrálně pomocí technologie Group Policy.

Lokální SMB keš se tedy zapíná a vypíná pro celý počítač jednorázově. Lokální SMB keš se nazývá offline files. Pod tímto názvem ji mohou znát i uživatelé, byť celkově je snaha GUI uživatelskou viditelnost této vlastnosti pokud možno skrýt.

Jakmile jsou offline files zapnuty pro daný počítač SMB klienta (SMB redirectoru), uživatel si může označovat jednotlivé soubory, dané jejich přesnou UNC cestou, ke kešování na lokálním disku. V principu, lokální keš může obsahovat pouze jednotlivé UNC soubory, nemůže obsahovat adresáře. UNC adresáře je sice možné také označit, aby byly dostupné offline, což ale ve skutečnosti způsobí pouze automatické označení všech jednotlivých jejich aktuálních souborů. Soubory, které v daném UNC adresáři přibydou později, budou nakešovány až v okamžiku, kdy se k nim později přistupuje, případně až se provede ruční synchronizace obsahu.

Síťové SMB soubory, dané svou UNC cestou, jsou kešovány do lokálního adresáře %windir%\CSC. CSC je zkratkou pro Client Side Cache. Tento adresář musí být na NTFS lokálním diskovém oddíle. Umístění tohoto adresáře je možno změnit v registrech počítače SMB klienta. Tato administrativní akce není ovšem příliš běžná, zvláště u stanic, kde se mnohdy nevyskytuje jiný lokální diskový oddíl naformátovaný na NTFS.

3.8. Online vs. offline práce s nakešovanými soubory offline files

SMB redirector automaticky sleduje dostupnost UNC cest. Na Windows XP a Windows 2003 sledoval SMB redirector dostupnost pouze celého host name (host header) UNC cesty – tedy dostupnost serveru, na kterém byly sdílené soubory přístupné. Od Windows Vista a Windows 2008 sleduje SMB redirector dostupnost pro každý označený UNC soubor zvlášť.

Pro přehlednost si popišme průběh práce s offline files.

a) na začátku si představme, že se uživatel připojí online k nějakému UNC síťovému SMB prostředku a pracuje s jeho soubory online. Tzn. SMB redirector má navázané TCP spojení s daným SMB serverem. Každé čtení je provedeno přes dané TCP spojení online, každý zápis jde přes síť přímo do skutečnéhost sdíleného souboru.
b) pokud SMB spojení spadne v průběhu čtení, nebo zápisu, tedy v průběhu nějaké IO operace nějaké klientské aplikace, tato se to dozví jako chybu čtení, nebo zápisu apod. Pravděpodobně pak informuje uživatele, že operace selhala a nechá ho vybrat opravu. Uživatel nejspíš může obvykle zvolit nový pokus o zápis, nebo čtení, který možná uspěje, pokud se podaří SMB spojení znovu obnovit
c) později se uživatel může rozhodnout jednotlivý UNC soubor označit, že má být dostupný offline. Zopakujme, že vždy v podstatě označujete jednotlivé UNC soubory, i když tak činíte pro celou složku. Uživatel nemusí označit všechny soubory z nějaké složky. Může označit pouze jeden, nebo jen několik takových souborů
d) v okamžiku kdy je nějaký soubor označen, začne SMB redirector na pozadí soubor synchronizaovat do lokální keše počítače v adresáři CSC. Dokud soubor není kompletně nakešován, chová se k němu SMB redirector stejně, jako by soubor nakešován nebyl vůbec
e) v okamžiku, kdy je soubor přítomen v CSC keši, SMB redirector poněkud pozmění své chování k operacím čtení a zápisu a zámkům výhradního přístupu na tento soubor

   a. soubory, které nejsou dostupné v lokální keši, nejsou vidět ani ve výpisu sdílených UNC adresářů v případě, že daný adresář není zrovna online k dispozici
   b. při ztrátě konektivity na sdílený prostředek zobrazuje SMB redirector lokálně pouze nakešované soubory a také pouze tyto soubory v zobrazení výpisů adresářů

f) SMB redirector si pamatuje u každého nakešovaného souboru navíc datum jeho poslední synchronizace, tedy datum, kdy se soubor naposledy změnil ve svém skutečném úložišti na UNC cestě.
g) operace přístupu k nakešovanému UNC souboru, se SMB redirector snaží vždy uspokojit online, pokud je SMB spojení možné. To znamená, že v případě zápisu do kešovaného souboru zapisuje sériově jak do jeho online UNC rodiče, tak i do své lokální kešované kopie. Stejně tak se chová k zámkům výhradního přístupu, kdy zamyká jak online soubor, tak i jeho kešovanou kopii
h) pokud spojení není možné, nebo spadne v průběhu dané IO operace, transparentně tuto opraci provede jen z/do lokální CSC keše a poznačí si, že se soubor změnil offline.
i) SMB redirector využívá také faktu, že má k dispozici lokální kopii souboru v případě čtení, i v případě, že je soubor dostupný v daném okamžiku online a pokud se nezměnila jeho časová razítka od poslední synchronizace, může uspokojit čtecí IO operaci z lokální CSC keše rychleji, než stahováním stejných dat ze sítě.
j) jak již bylo řečeno, SMB redirector se snaží při každém přístupu k souboru s ním pracovat online. Tím pádem, pokud dojde k obnovení konektivity v libovolně krátkém/dlouhém čase od posledního offline přístupu, SMB redirector se velmi rychle dozví.
k) pokud dojde k obnovení spojení a soubor je nyní znovu k dispozici online, SMB redirector porovná jeho časová razítka v lokální CSC keši a na vzdáleném SMB serveru.
   a. pokud se soubor nezměnil ani na SMB serveru, ani lokálně v keši offline, nic se neděje

b. pokud se soubor změnil mezitím na SMB serveru a přitom se nezměnil lokálně v keši, je opět považován za nezesynchronizovaný a na pozadí začne probíhat jeho synchronizace, zatímco jeho IO operace probíhají kompletně pouze online
c. pokud se soubor změnil mezitím pouze v lokální offline CSC keši, SMB redirector započne na pozadí jeho zpětnou synchronizaci z keše do online UNC souboru s tím, že cílový soubor zamkne výhradně pro svoji potřebu. Po dobu jeho synchronnizace do online UNC cesty vykonává SMB redirector všechny klientské IO operace pořád ještě lokálně do své offline kopie souboru.
d. pokud se soubor po dobu výpadku konektivity změnil na obou místech, tedy jak v lokální CSC keši, tak i na online UNC cestě, nemůže SMB redirector sám provést synchronizaci. Takový soubor je potom i nadále považován za offline a veškeré přístupy k němu jsou transparentně pouze lokální, do lokální keše CSC. Uživatel musí sám použít ovládací panely Synchronizace k tomu, aby konflikty ručně vyřešil.

l) z uvedeného plyne, že je možné, že za určitých okolností bude mít uživatel na stanici množství pozměněných souborů v lokální CSC keši, které budou paralelně měněny na své UNC cestě někým jiným. V takové situaci bude muset uživatel provést kvalifikovaný, ruční, zásah do synchronizace pomocí ovládacího panelu a vyřešit určitý počet konfliktů vlastnoručně.

Technologie offline files umožňuje samozřejmě manuální vynucení synchronizace všech souborů. Taková synchronizace se dá i naplánovat na různé časové intervaly, nebo na uživatelem vyvolané události, jako je například zamknutí pracovní plochy, nebo delší doba nečinnosti.

Důležité je uvědomit si chování offline files z pohledu uživatele. Pokud si uživatel nějaké soubory označí, že mají být dostupné offline, může s nimi transparentně pracovat na jejich normální UNC cestě i když ve skutečnosti nemá konektivitu s daným SMB serverem. Ostatní soubory z daného SMB serveru, které

nebyly označeny pro offline dostupnost, nebudou na UNC cestě ani vidět ve výpisu adresáře, ani logicky dostupné pro IO operace.

Vzhledem k tomu, že funkce mapování disku na UNC cestu je záležitostí vyšší úrovně, než je offline files keš SMB rediretoru, uživatelé si mohou označovat pro kešování i soubory na mapovaných discích. Mapované disky také zůstanou normálně přístupné i offline, pakliže obsahují alespoň jeden nakešovaný soubor.

3.9. Formát CSC lokální keše a jeho bezpečnost a okrajové podmínky

Obsah adresáře CSC je nedokumentovaný ze strany Microsoft. Souboru v něm není možné jednoduše identifikovat ani jejich počet, ani jejich obsahy nemusí být přímo obrazem kešovaných souborů. Tzn. neplatí, že jeden soubor v CSC, byť přejmenovaný, rovná se zdrojový UNC soubor. Data kešovaných souborů jsou zde ovšem uložena nezašifrovaně, tudíž definitivně v rekonstruovatelné formě.

Z tohoto důvodu jsou zde keše oddělené pro jednotlivé uživatele. Keše jednotlivých uživatelů je možno nechat zašifrovat pomocí EFS. Tím je možné oddělit nakešované soubory jednotlivých uživatelů od sebe navzájem a současně od správců stanic.

Pokud by si dva různí uživatelé nechali nakešovat stejný UNC soubor, bude tento v CSC keši uložen skutečně dvakrát.

Maximální velikost CSC keše pro celý počítač je možno omezit na velikost například v GB. Ve výchozím stavu je její velikost omezená pouze volným místem na disku, na kterém se tento CSC adresář nachází.

Offline files automaticky spravují místo v CSC keši a pokud místo dochází, automaticky, bez hlášení keš uvolňují a odstraňují nakešované soubory, které nebyly offline změněny od jejich poslední synchronizace.

Soubory v CSC keši si SMB redirector identifikuje pomocí jejich přesné UNC cesty. Pokud by uživatel přistupoval na jeden SMB server na jeden jeho UNC soubor pomocí více různých UNC cest (různé DNS FQDN aliasy, různá jména SMB

serveru, krátké vs. dlouhé jméno, IP adresy apod.), budou se různé takové UNC prostředky jevit, jako buď nakešované a dostupné offline, nebo nedostupné. Tedy podle toho, jakou přesně UNC cestu si uživatel označil, bez ohledu na to, že se jedná o fyzicky stejný sdílený soubor.

Jako příklad uveďme, že z pohledu SMB redirectoru jsou například i tyto dvě UNC cesty \\fileserver\Faktury\fakt0034053.pdf a \\fileserver.ad.jcu.cz\Faktury\fakt0034053.pdf rozdílné a tudíž je možné, že jedna bude dostupná offline, zatímco druhá nebude.

Stejně tak, pokud by uživatel offline modifikoval onen stejný soubor offline přes obě dvě UNC cesty, které si označil offline k dispozici, bude se jednat o dvě nezávislé modifikace v principu dvou různých lokálních kešovaných souborů. Po opětovném obnovení konektivity pak vznikne konflikt na jediném skutečném online UNC prostředku.

4. Závěr

Offline files jsou automaticky zapnuté na počítačích zaměstnanců pro přesměrované složky (folder redirection). To tedy znamená, že všichni uživatelé pracující na počítačích zaměstnanců, by měli mít ve výchozím stavu, kešované celé obsahy UNC cest, do kterých jsou přesměrovány jejich složky Dokumenty a Plocha. Uživatelé si mohou tuto funkci sami vypnout na úrovni jednotlivých souborů, nebo podsložek.

Vzhledem k tomu, že takto jsou označeny celé tyto složky, znamená to, že každý soubor, který do nich uživatelé sami uloží se automaticky nakešuje. Stejně jako všechny soubory, ke kterým z těchto složek uživatelé přistupují.

Pokud mají uživatelé více počítačů a tím pádem do těchto složek ukládají a modifikují soubory z jednoho stroje, jeho keš se aktualizuje. Zatímco keš druhého jejich počítače se sama neaktualizuje, pokud s nějakým souborem nepracují.

Z tohoto důvodu mají počítače zaměstnanců centrálně zapnutu manuální synchronizaci těchto složek a naplánovánu na okamžiky přihlášení, odhlášení a delší nečinnosti.

Pro cestovní profily nemá použití offline files smysl.

Pro domovský adresář (a tedy jeho UNC cesty) si uživatelé musí dostupnost offline řídit sami ručně. Mohou si ji nastavit na úrovni jednotlivých souborů, nebo celých podadresářů svého domovského adresáře.

Za několikaměsíční dobu ostrého provozu jsem narazil na jeden problém u jednoho konkrétního notebooku, kdy měl chybu na pevném disku a občas se vrátil do předchozího bodu obnovení, tudíž se vrátil v čase. Následně byl notebook automaticky vyjmut z domény a synchronizace se pozastavila do doby opětovného připojení.

5. Seznam obrázků

6. Seznam tabulek

7. Použité zdroje

Dropbox. Wikipedia [online].2013 [cit. 2014-04-19]. Dostupné z: http://cs.wikipedia.org/wiki/Dropbox

Get more space. Dropbox [online]. 2014 [cit. 2014-2-5]. Dostupné z: https://www.dropbox.com/getspace

Upgrade to Dropbox Pro. Dropbox [online]. 2014 [cit. 2014-03-04]. Dostupné z: https://www.dropbox.com/upgrade

DropBox. DropBox [online]. 2014 [cit. 2014-03-04]. Dostupné z: http://www.dropbox.cz/web/cenik-programy.html

Terms of Service. Dropbox [online]. 2014 [cit. 2014-03-25]. Dostupné z: https://www.dropbox.com/terms#terms

Google Drive. Wikipedia [online]. 2012 [cit. 2014-1-2]. Dostupné z: http://en.wikipedia.org/wiki/Google_Drive

Storage Plan Pricing. Support Google [online]. 2014 [cit. 2014-04-10]. Dostupné z: https://support.google.com/drive/answer/2375123?hl=cs

Smluvní podmínky společnosti Google. Google [online]. 2014-4-14 [cit.2014-04-20]. Dostupné z: http://www.google.com/policies/terms/

OneDrive. Wikipedia [online]. 2014 [cit. 2014-04-20]. Dostupné z: http://en.wikipedia.org/wiki/OneDrive

Microsoft Officially Rebrands SkyDrive To OneDrive. Techcrunch [online]. 2014-02-19 [cit. 2014-04-01]. Dostupné z: http://techcrunch.com/2014/02/19/microsoft-officially-rebrands-skydrive-to-onedrive/

Správa úložiště. OneDrive [online]. 2014 [cit. 2014-04-15]. Dostupné z: https://onedrive.live.com/Options/ManageStorage?ru=https%3a%2f%2fonedrive.live.com%2f%3fgologin%3d1%26mkt%3dcs-CZ

Upgrade options. OneDrive [online]. 2014 [cit. 2014-04-03]. Dostupné z: https://onedrive.live.com/Options/Upgrade?ru=https%3a%2f%2fonedrive.live.com%2f

OneDrive. Wikipedia [online]. 2014 [cit. 2014-04-20]. Dostupné z: http://en.wikipedia.org/wiki/OneDrive

Timeline of Microsoft Windows. Wikipedia [online]. 2014-02-18 [cit. 2014-04-10]. Dostupné z: http://en.wikipedia.org/wiki/Timeline_of_Microsoft_Windows

RUSSINOVICH, Mark E, David A SOLOMON a Alex IONESCU. Windows internals. 6th ed. Redmond: Microsoft Press, 2012, xxii, 726 s. ISBN 978-0-7356-4873-9.

RUSSEL, Charlie a Sharon CRAWFORD. MICROSOFT. *Microsoft Windows Server 2008: velký průvodce administrátora*. Vyd. 1. Brno: Computer Press, 2009, 1271 s. Administrace (Computer Press). ISBN 978-80-251-2115-3.

8. Přílohy

1. Tato bakalářská práce ve formátu pdf.