Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Active Directory v moderním IT

Bc. Jan Bílek

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Active Directory v moderním IT" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 23.11.2017 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D. za jeho konzultace a vedení mé práce. Dále také rodině a všem, kteří mi poskytli podporu při psaní této práce.

Active Directory v moderním IT

Souhrn

Diplomová práce „Active Directory v moderním IT“ se zabývá adresářovou službou Active Directory od společnosti Microsoft a jejím současným vývojem v prostředí cloudových služeb. Cílem práce není obecná charakteristika cloudových služeb jako celku, ale pouze komponent spojených s adresářovou službou Active Directory, tyto komponenty jsou však stavebním kamenem většiny dalších cloudových služeb, protože služba Active Directory obvykle poskytuje těmto službám možnost autentizace, autorizace a případně jednotného ověřování (Single Sign On).

Služba Active Directory, ačkoliv byla představena v roce 1999, je založena na technologiích pocházejících z počátku 70. let 20. století a nebyla zamýšlena pro použití v prostředí internetu. Trendem v moderním IT je však využívání cloudových IT služeb a tomuto trendu se musela přizpůsobit i služba Active Directory.

Praktická část této práce řeší příklad z praxe – využití služeb Active Directory použitých v lokální síti firmy v souvislosti s použitím cloudových služeb.

Klíčová slova: Active Directory, Cloud, Single Sign On, Autentizace, Microsoft, Kerberos, LDAP

Active Directory in modern IT

Summary

Active Directory in modern IT thesis describes Active Directory directory service from Microsoft company and its current development in area of cloud services. Goal of this thesis is not to generally describe cloud services from wide point of view, but describes only components regarding directory services - Active Directory. These components are however corner stones of most of cloud services as they are often using Active Directory as a service providing authentication, authorization and Single Sign on functionality.

Active Directory directory service, however it was introduced in 1999, is based on technology from early 1970s and was not basically intended to be used in internet environment. Trend in modern IT however is, to use cloud IT services and Active Directory had to be adjusted so it can be used in this environment.

Practical part of this thesis describes using Active Directory in real world scenario – using on-premise Active Directory service to authenticate cloud services.

Keywords: Active Directory, cloud, Single Sign On, authentication, Microsoft, kerberos, LDAP

Obsah

1. Úvod

Služba Active Directory, ačkoliv byla představena v roce 1999, je založena na technologiích pocházejících z počátku 70. let 20. století a nebyla zamýšlena pro použití v prostředí internetu. Služba Active Directory nejčastěji fungovala jako centrální správce identit a umožňovala řízení přístupu ke zdrojům uvnitř lokální počítačové sítě.

Postupem času a s rozšířením internetu vznikla potřeba přistupovat k firemním datům vzdáleně přes internet. Nejčastěji přes VPN připojení do interní sítě.

Trendem v moderním IT je však využívání cloudových služeb, uživatelé již nepracují jen z kanceláře, chtějí pracovat odkudkoliv, využívat několik zařízení, pevný počítač, notebook, tablet, chytrý mobilní telefon atd. Tomuto trendu se musela přizpůsobit i služba Active Directory a tak se její součástí stala i služba federace identit – Active Directory Federation Services, která podobné scénáře nasazení umožňuje.

Teoretická část práce zavádí pojmy Adresář, Adresářová služba, protokol pro přístup k adresářové službě - Lightweight Directory Access Protocol (dále jen LDAP), Kerberos, Single Sign On, jakožto klíčové pojmy technologie Active Directory. Dále teoretická část popisuje službu Active Directory Federation Services, která je využívána pro spojení vnitřního Active Directory s cloudovými službami.

Praktická část této práce se věnuje scénářům z praxe – využití ověřovacích služeb Active Directory použitých v lokální síti firmy v souvislosti s použitím cloudových služeb, kde autor simuluje situaci z praxe, ve které se společnost rozhodne pro využití cloudové služby jako doplňku ke službám poskytovaným v lokální síti a následně stojí před otázkou jak co nejelegantněji vyřešit ověřování uživatelů.

Druhý scénář z praxe simuluje situaci, kdy se společnost rozhodne sdílet svá data s jinou společností, ať už kvůli práci na stejném projektu, nebo například kvůli následnému sloučení obou společností. Stejně jako v prvním případě je nutné vyřešit otázku ověřování uživatelů pomocí metody Single-Sign-On, tak aby uživatel mohl používat jedinou sadu přihlašovacích údajů.

Oba scénáře jsou nasimulovány v laboratorním prostředí.

2. Cíl práce a metodika

2.1 Cíl práce

Cílem práce je charakterizovat službu Active Directory, a to konkrétně její logickou i fyzickou architekturu, její historii, vývoj a následně její nasazení v podmínkách moderního IT představovaného cloudovými službami. Poukázat na rozdílné principy autentizace používané v prostředí moderního IT a jejich výhody a nevýhody. Řešení bude zaměřeno s ohledem na technologii, ale i ekonomiku celého řešení.

Cílem praktické části je nasazení služby Active Directory pro ověřování uživatelů cloudové služby v laboratoratorním prostředí a ověření náročnosti nasazení jednotlivých principů autentizace v praxi.

2.2 Metodika

Metodika řešení problematiky diplomové práce je založena na studiu informačních zdrojů, zejména technické literatury o architektuře a návrhu řešení se službou Active Directory. Poznatky ze studia formulují Teoretická východiska. Teoretická východiska poskytují úvod do technologií adresářových služeb, popisují technologii Active Directory a její komponenty a dále uvádí do historického kontextu technologii federace identit ADFS (Active Directory Federation Services) používanou při autentizaci v moderním IT.

Praktická část je založena na vytvoření laboratorního prostředí založeného na virtualizované IT infrastruktuře fiktivních společností. Laboratorní prostředí simuluje situaci z praxe, ve které se společnost rozhodne pro využití cloudové služby jako doplňku ke službám poskytovaným v lokální síti a stojí před rozhodnutím o volbě autentizační technologie.

Do laboratorního prostředí jsou následně nasazeny všechny zamýšlené varianty autentizace uživatelů. Navrhovaná řešení jsou dále zkoumána z pohledu nákladů na jednotlivá řešení a složitosti jejich nasazení.

Na základě analýzy výsledků je potom formulován závěr práce.

3. Teoretická východiska

3.1 Adresářové služby a LDAP

Tato kapitola obsahuje teoretický úvod do problematiky adresářové služby a protokolu LDAP, který je použit jako klíčová komponenta adresářové služby Active Directory.

3.1.1. Adresář

Adresář (anglicky „directory“) je určitou formou databáze. Data jsou uložena ve formě hierarchické struktury. Adresářová databáze obsahuje informace o objektech v síti. Objektem může být uživatelský účet, počítačový účet, tiskárna, případně služba, ale také skupina, do které jsou objekty organizovány. Na rozdíl od relační databáze je adresář optimalizován pro čtení a vyhledávání, a ne pro zápis. V adresáři je možné ukládat různé typy dat jako například textová data, digitální certifikát, případně obrázek. Přístup k záznamům v adresáři můžeme upravit nastavením ACL (Access Control List) záznamů, podobně jako je to u souborů na souborovém systému.

3.1.2. Adresářová služba

Adresářová služba (anglicky „directory service“) je úložiště informací, které slouží jako kontaktní bod, pomocí kterého mohou uživatelé nebo aplikace vyhledat služby a objekty distribuované v síti. Adresářové služby přistupují k adresáři. Adresářová služba také funguje jako centrální autorita pro autentizaci, která umožňuje věrohodnou autentizaci objektů v síti – například autentizaci uživatele při přístupu ke sdílenému souboru na souborovém serveru. Active Directory (AD) firmy Microsoft je typickým příkladem adresářové služby. AD využívá protokol LDAP a vyhovuje standardu LDAP v3 popsaném v RFC 3377.

3.1.3. LDAP

Lightweight Directory Access Protocol (zkráceně LDAP) je aplikační protokol pro komunikaci s adresářovými službami. Protokol LDAP využívá TCP/IP. LDAP vznikl jako zjednodušení protokolů X500, které vznikly v 80. letech 20. století. LDAP využívá LDAP Data Interchange Format (LDIF), což je standardní formát výměny dat. Data jsou při přenášení zakódována. Zakódována jsou pomocí Lightweight Basic Encoding Rules (zkráceně LBER). LBER ale nelze považovat za bezpečnostní šifru, a proto není složité data dekódovat.

LDAP sestává ze čtyř modelů, jimiž se zabývají následující odstavce.

- informační model – schéma,
- jmenný model,
- funkční model,
- bezpečnostní model.

3.1.4. Informační model – schéma

Informace v adresáři jsou uloženy v Directory Information Tree (DIT), což je stromová struktura. Z tohoto důvodu je také databázový soubor Active Directory pojmenován s příponou DIT. Informační model je složen ze záznamů, které reprezentují nějakou entitu z reálného světa – například uživatel nebo počítač. V prostředí Microsoft Active Directory se LDAP záznamy nazývají objekty. Objekty sestávají z množství atributů (např. jméno, příjmení, e-mail), které mají vždy daný typ a jednu případně více hodnot. Implementací informačního modelu je schéma, což je množství objektů, definujících strukturu a atributy každého objektu, který může být vytvořen v adresářové službě. Schéma tedy zavádí všechny třídy objektů, které je možno v adresářové službě použít, a definuje jejich obsah (atributy). Původní schéma pro určitou adresářovou službu je možno rozšířit, například při instalaci poštovního serveru Exchange do prostředí AD je nutné rozšířit výchozí schéma dalšími atributy potřebnými pro poštovní služby.

Třídy objektů jsou obecné kategorie objektů, které je možné vytvořit v adresářové službě. V protokolu LDAP se využívá označení objectClass a například to může být třída user, computer, organizationalUnit, domain, container, group. Třídy objektů jsou zařazovány do jedné ze třech kategorií Abstract, Auxiliary nebo Structural. Objekt v Active Directory smí být zařazen současně do více tříd. Příkladem je uživatel, který je zařazen do tříd user, top, person, organizationalPerson. nebo počítač, který je v třídách computer a top, person, organizationalPerson, user.

Atributy objektů jsou určité vlastnosti objektů v adresáři. Atribut může obsahovat jednu nebo také více hodnot, například jméno, příjmení, adresu, telefon, e-mail. Určité atributy patří k určité třídě objektů a schématem je definováno, jaké hodnoty jsou povinné a jaké jsou volitelné. Schéma také definuje, jaké typy hodnot smí atribut nabývat, může to být například

textový řetězec, celé číslo. V adresářové infrastruktuře Active Directory existuje specifický doménový řadič zodpovědný za správu schématu.

Podle polohy objektu ve stromové struktuře se jedná buď o list, který nemá žádné potomky, nebo o kontejner, který může obsahovat jeden či více objektů. Příklad atributů objektů Active Directory znázorňuje následující tabulka:

Atribut	**Popis**
givenName	Křestní jméno
sn	Příjmení
mail	e-mailová adresa
displayName	Zobrazované jméno
company	Jméno společnosti
department	Název oddělení

Tabulka 1- Příklad atributů objektů Active Directory (1)

3.1.5. Jmenný model

Jmenný model popisuje organizaci a odkazování informací v adresáři. Pro identifikaci objektů v adresáři je použito Distinguished Name (DN)**,** které obsahuje úplnou cestu k záznamu a zároveň daný objekt jednoznačně identifikuje. DN je složeno ze samotného jména objektu a dále ze jmen jednotlivých organizačních jednotek, případně kontejnerů a domén, které daný objekt obsahují, oddělených čárkou. Jednotlivé položky obsahují název jmenného atributu a jeho přiřazenou hodnotu, třeba ou=zamestnanci**.**

Například v organizační jednotce *zaměstnanci* domény czu.cz je umístěn uživatel Jan Novák, pro kterého je výsledné DN = cn=Jaromír Mrkvička,ou=zamestnanci,dc=czu,dc=cz.

Relative Distinguished Name (RDN) je na rozdíl od DN relativní a jednoznačné v daném kontejneru. Jedná se o poslední část DN, pro našeho uživatele je RDN = cn= Jaromír Mrkvička.

Běžnou identifikací objektu pomocí protokolu LDAP a také v Active Directory je Distinguished Name, ale používají se i další metody speciálně pro Active Directory. Můžeme použít Object Identifier (OID), což je unikátní hierarchický identifikátor složený z číslic oddělených tečkou. V Active Directory má každý objekt přiřazen jednoznačné 128bitové číslo, které se označuje globally unique identifier (GUID). Toto unikátní číslo je stálé a nemění se při přesunu objektu. Active Directory také používá obdobu Distinguished Name, která se

označuje jako canonical name(CN), které nese stejnou informaci jako DN, ale je zapsáno pomocí DNS zápisu, příkladem je zápis czu.cz/zamestnanci/Jaromír Mrkvička

3.1.6. Funkční model

Funkční model v protokolu LDAP definuje funkce dostupné pro práci s informacemi v adresáři. LDAP zahrnuje funkce pro autentizaci, dotazování a vyhledávání.

3.1.7. Bezpečnostní model

Bezpečnostní model protokolu LDAP definuje způsob přístupu k datům z bezpečnostního pohledu. Souvisí s autentizací a autentizačními službami z adresářových služeb.

3.2 Active Directory Domain Services

Active Directory (AD) je adresářová služba od společnosti Microsoft. Active Directory Domain Controller (DC či doménový řadič) je server, na kterém běží Active Directory Domain Services (AD DS, tento název je použit od Windows Server 2008, předtím se používal název Active Directory a ve Windows NT potom Domain Services). AD DS poskytuje distribuovanou databázi, která v hierarchické struktuře obsahuje objekty (jako je například uživatel, počítač, skupina). Zajišťuje také autentizaci a autorizaci uživatelů a počítačů v síti. Využívá LDAP protokol rozšířený o protokol Kerberos verze 5 a DNS (Domain Name System). Pro správu AD DS se využívají nástroje pro správu serverů (Remote Server Administration Tools), například Active Directory users and computers, Active Directory domains and trusts atd.

3.2.1. Doména a strom domén

Doména (Domain) je logická skupina počítačů, která využívá společnou AD databázi.

Logická struktura služby Active Directory je postavena na konceptu domén. Domény byly zavedeny už v systému Windows NT 3.x a 4.0. Nicméně teprve s příchodem Windows 2000 a technologie Active Directory byly domény významně aktualizovány z ploché a nepružné struktury dané systémem Windows NT na vysoce výkonné a škálovatelné řešení.

Doména Active Directory se skládá z následujících komponent:

- hierarchická struktura kontejnerů a objektů založená na standardu X.500,

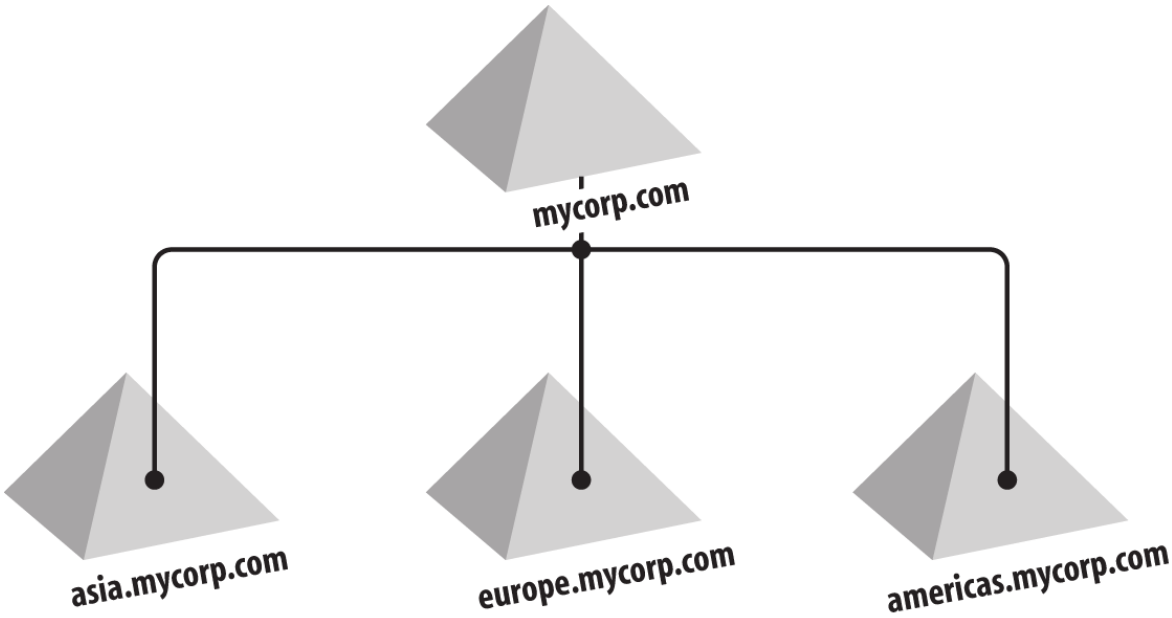
- DNS název domény jako její jedinečný identifikátor,
- bezpečnostní služba, která ověřuje a autorizuje přístupy ke zdrojům prostřednictvím účtů v doméně nebo vztahu důvěryhodnosti (Trustu) s ostatními doménami,
- politiky, které určují, jak je upravena funkčnost systému pro uživatele nebo zařízení v rámci této domény.

Řadič domény (DC) může být autoritativní pro jednu a pouze jednu doménu. Není možné hostovat více domén na jednom řadiči domény Active Directory. Například fiktivní společnost Mycorp již má přidělen název domény DNS pro svou společnost s názvem mycorp.com, a tak se rozhodne, že první doména Active Directory se bude jmenovat „mycorp.com“. Mycorp.com je tedy kořen stromu domén.

Doména mycorp.com sama o sobě, bez ohledu na její obsah, je v tomto případě automaticky vytvořena jako kořen z hierarchické struktury zvané strom domény. Jedná se o hierarchický systém domén, přičemž všechny domény v tomto sytému používají souvislý systém pojmenování. Pokud společnost Mycorp přidá další domény zvané například Evropa, Asie a Americas, pak jména domén budou: europe.mycorp.com, asia.mycorp.com a americas.mycorp.com. Každý strom domény se nazývá podle kořenové domény, proto tento strom bude označen mycorp.com. Obrázek 1 – Doménový strom - Mycorp.com znázorňuje graficky strom mycorp.com.

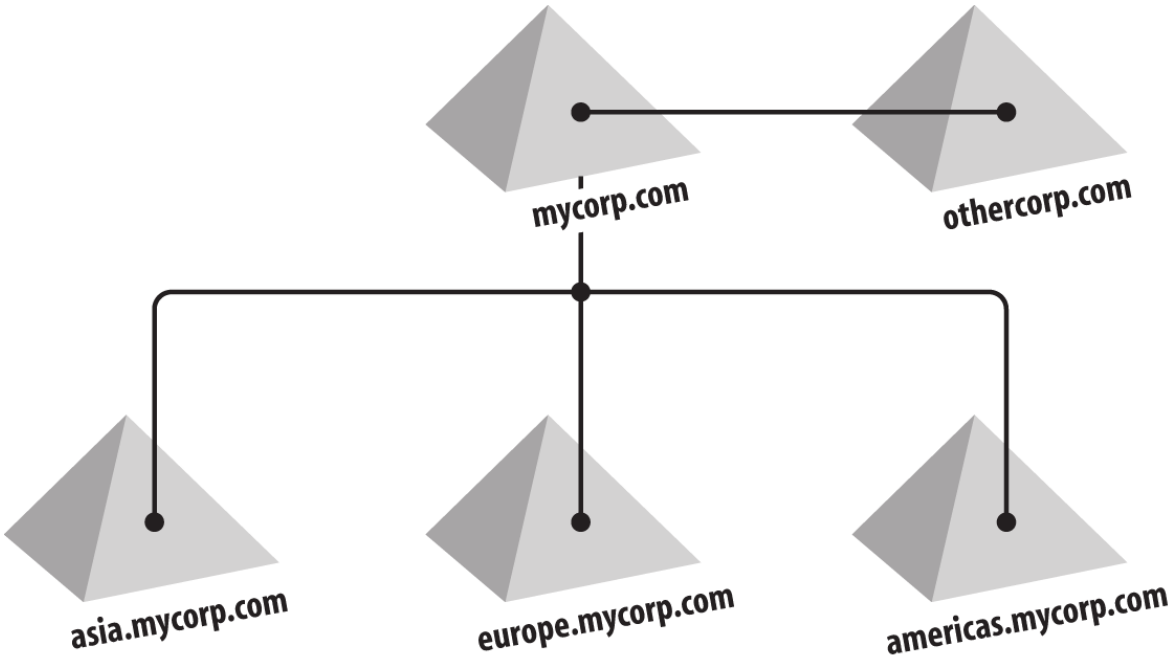
V případě stromu Mycorp.com je patrná souvislá řada domén, které jsou uspořádány do úhledného stromu.

V případě, že by prostředí obsahovalo jedinou doménu, stále by se tato topologie označovala jako doménový strom, i když fakticky pouze s jednou doménou.



Obrázek 1 – Doménový strom - Mycorp.com (2)

Stromy domén usnadňují správu a přístup ke zdrojům, protože všechny domény ve stromu si implicitně vzájemně důvěřují prostřednictvím transitivních trustů (vztahy důvěryhodnosti mezi doménami). Transitivita trustu znamená, že pokud důvěřuje doména A doméně B a doména B důvěřuje doméně C, znamená to, že Doména A důvěřuje zároveň i doméně C. To je znázorněno na obrázku 2. V praxi to znamená, že například správce domény asia.mycorp.com může umožnit každému uživateli v doménovém stromu přístup na kterýkoliv zdroj (soubor, intranet atd.) v asia doméně. Uživatel nemusí být ve stejné doméně, aby mohl získat přístup k danému zdroji.



Obrázek 2- Doménový strom mycorp.com se vztahem důvěryhodnosti (2)

Jméno Active Directory domény je běžně plně kvalifikované doménové jméno (Fully qualified domain name). Může obsahovat písmena, číslice, pomlčku; tečku smí obsahovat pouze pro oddělení komponent. Maximální délka názvu je 64 znaků. Každá doména má také jméno, které se označuje jako NetBIOS doménové jméno (příklad mycorp). To může mít maximálně 15 znaků a nemůže obsahovat tečku a některé další znaky. Pro zobrazení domén je možné použít nástroj AD Domains and Trusts, ve kterém je seznam domén a funkční level domény a funkční level lesa.

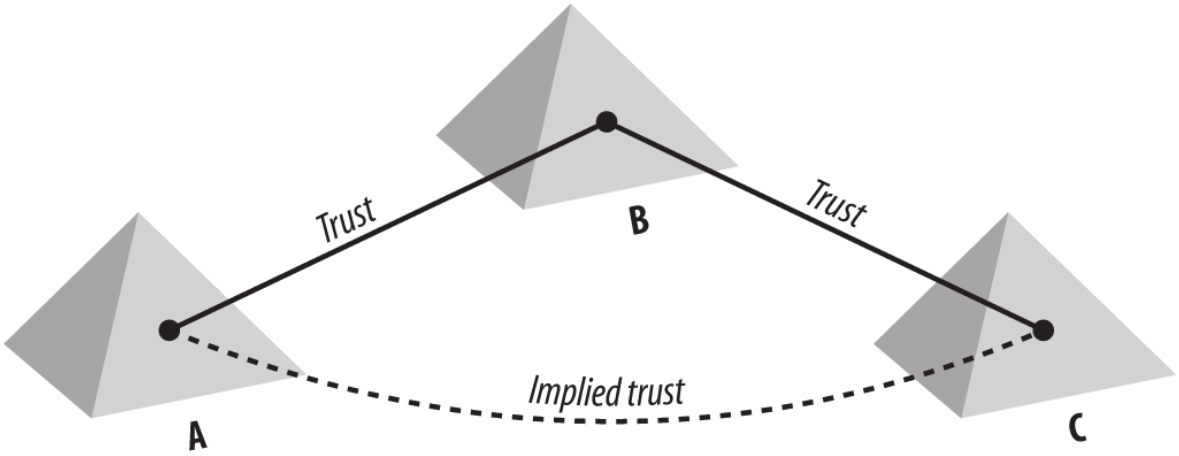
3.2.2. Les (Forest), schéma a vztahy důvěryhodnosti (Trusty)

Podobně jako je strom domén určitá skupina domén, les je skupina stromů domén. Tyto doménové stromy sdílí společné schéma a konfigurační část domén. Stromy jako celek jsou vzájemně propojeny přes transitivní vztahy důvěryhodnosti. Jakmile je vytvořena i jen jediná prázdná doména, z logického pohledu byl vytvořen strom domén a zároveň i les. Vytvořená doména je tedy kořenovou doménou stromu domén a zároveň kořenovou doménou lesa. Jsou-li později přidány nějaké další domény do původního stromu domény nebo celé nové stromy domén, stále se z logického pohledu bude jednat o jeden les.

Les je pojmenován po první doméně, která je vytvořena. Tato doména je známá jako kořenová doména lesa (Forest root domain). Kořenová doména je pro samotný forest velmi důležitá. V případě služby Active Directory není možné odstranit kořenovou doménu lesa; při odstranění kořenové domény je nenávratně zničen celý les. Windows Server 2003 a novější verze Active Directory nabízí možnost přejmenovat kořenovou doménu lesa, ale nelze změnit její stav jako kořenové domény nebo udělat z jiné domény kořenovou.

Rozviňme příklad s fiktivní společností Mycorp. Společnost Mycorp má dceřinnou společnost s názvem Othercorp. Název domény DNS přidělený a použitý společností Othercorp je „othercorp.com“. Vše, co je třeba udělat v tomto případě, je vytvořit kořen stromu domén othercorp.com jako člen existujícího lesa mycorp.com. Společnosti Othercorp.com a Mycorp.com potom budou moci společně komunikovat a sdílet zdroje, jak je znázorněno na obrázku 3.

Les obsahující mycorp.com a othercorp.com doménové stromy poté vystupuje jako les s názvem mycorp.com, ve kterém mycorp.com je kořenová doména.



Obrázek 3- Transitivní trust (2)

Zatímco více doménových stromů v lese může být nakonfigurováno, je nutné vážně zvážit všechny důsledky takového uspořádání před implementací. Ve výsledku takováto konfigurace může být matoucí při řešení případných problémů, když se pracuje na problému v othercorp.com doméně, ale konfigurační informace jsou udržovány v oddílu cn=configuration,dc=mycorp,dc=com.

I když existují oprávněné důvody k vytvoření tzv. multitree lesů, je obecně doporučeno usilovat o to, aby byl návrh Active Directory jako celku, pokud možno co nejjednodušší a pokud možno se omezil pouze na jeden doménový strom a co nejméně domén.

Osvědčené postupy (best practice) pro nové implementace Active Directory téměř vždy radí vytvořit forest s pouze jedinou doménou. V této části diplomové práce jsou nastíněny různé možnosti návrhu pro demonstraci konceptu domén, stromů domén a lesů, nicméně praktická implentace této technologie závisí na mnoha okolnostech, a ne vždy může navržený koncept být ideální.

Jednotlivé společnosti obvykle používají své vlastní lesy domén Active Directory. Pokud by tedy společnost Othercorp používala svůj vlastní les domén Active Directory, bylo by nutné vytvořit vztah důvěry (forest trust) mezi lesem Mycorp a lesem Othercorp tak, aby bylo možné poskytnout jednotný přístup ke zdrojům mezi oběma společnostmi.

Vztah důvěryhodnosti mezi lesy (forest trust) umožňuje správci vytvořit tranzitivní jednosměrný nebo obousměrný vztah důvěryhodnosti (trust) mezi dvěma kořenovými doménami. Tento trust umožňuje, aby všechny domény v jednom lese důvěřovaly všem doménám v druhém lese a naopak.

V případě obchodních nebo organizačních jednotek, které jsou nezávislé, a ve skutečnosti si přejí být izolovány od sebe navzájem, není možné je spojit do jediného lesa. Pokud si každá obchodní jednotka vytvoří v rámci lesa vlastní doménu, tyto obchodní jednotky jsou vedeny dojmem, že jsou autonomní a odděleny od sebe navzájem. Nicméně v Active Directory této úrovně autonomie a izolace lze dosáhnout pouze prostřednictvím samostatného lesa domén active directory (Active Directory Forest). To je také jediné řešení legislativních požadavků na izolaci.

3.2.3. Organizační jednotky

Domény, stromy a lesy jsou součástí obecného pohledu na Active Directory.

Další odstavec popisuje detailnější pohled na strukturu Active Directory. Při detailním pohledu do domény Active Directory je patrná hierarchická struktura objektů. Tato hierarchie se skládá z objektů, které mohou fungovat jako určitý kontejner a objektů, které nemohou fungovat jako kontejner. Primární typ kontejneru, který umožňuje vkládání objektů je organizační jednotka

(OU – Organizational Unit). Jiný typ kontejneru, který se ve skutečnosti nazývá taktéž kontejner, může být také použit pro uložení hierarchie objektů.

Ačkoli oba mohou obsahovat obrovské hierarchie jiných kontejnerů a objektů, organizační jednotka může být použita pro aplikace skupinových zásad (Group Policy), kontejner tuto možnost nemá a je obvykle používán pouze pro systémové objekty.

Z tohoto důvodu se organizační jednotky používají téměř výhradně jako stavební objekt hierarchie v rámci domény.

Například doména asia.mycorp.com z obrázku 2 má 500 uživatelů a 500 účtů počítačů. Většina běžné údržby uživatelů a počítačů je velmi jednoduchá, ale výrobní úsek v současné době prochází restrukturalizací a provádí rozsáhlý nábor zaměstnanců. Zaměstnanci jsou najímáni, případně přechází z jiných oddělení společnosti. Pro omezení zátěže administrátorů se společnost mycorp.com rozhodne dát vedoucím pracovníkům HR omezenou autonomii nad objekty uživatelů tím, že umožní jednomu z vedoucích správců řídit svou vlastní část stromu. V tomto příkladu není nutné úplné oddělení z důvodu bezpečnosti a příslušný strom není dost velký, aby ospravedlnil vytvoření další domény. Místo toho je možné vytvořit organizační jednotku v hierarchii a vedoucímu pracovníkovi HR následně delegovat oprávnění vytvářet a mazat účty, měnit hesla a případně vytvořit další organizační jednotky. Je zřejmé, že oprávnění, která má vedoucí pracovník HR dostat, musí být náležitě přizpůsobena tak, aby měl kontrolu pouze nad danou organizační jednotkou, a ne celou doménou.

Při instalaci Active Directory domény je vytvořena řada výchozích kontejnerů a organizačních jednotek automaticky včetně výchozích kontejnerů pro počítače, uživatele a řadiče domény.

3.2.4. Skupiny

Active Directory podporuje tři rozsahy skupiny: místní doménové skupiny (Domain Local), globální skupiny (Global) a univerzální skupiny (Universal). Každý rozsah skupiny se chová mírně odlišně v závislosti na funkční úrovni domény a funkční úrovně lesa. Každý rozsah skupiny se dále dělí na dva typy: distribuční a bezpečnostní skupina.

Pokud je skupina distribuční, neobsahuje SID (Security ID) identifikátor, a tedy tento identifikátor není přidán do tokenu zabezpečení uživatele při přihlášení. Z toho vyplývá, že tato skupina nemůže být použita pro účely zabezpečení ve Windows, například pro zřízení přístupu

ke sdílené složce. Distribuční skupiny jsou obecně používány jako distribuční seznam (skupina uživatelů, kterým můžete odeslat mail najednou), i když je možné je použít jako bezpečnostní skupiny pro aplikace na bázi protokolu LDAP nebo pro jiné aplikace, které nepoužívají standardní model zabezpečení systému Windows. Microsoft Exchange například používá distribuční seznamy s použitím distribučních skupin v Active Directory. Bezpečnostní skupiny, na rozdíl od distribučních, jsou načteny během přihlašování uživatele a SIDy těchto skupin, jejichž uživatel je členem, jsou přidány do tokenu zabezpečení uživatele. Skupiny zabezpečení lze ale také využít v případě Microsoft Exchange jako distribuční seznamy.

Všechny edice systému Windows, které podporují protokol Kerberos, mohou mít problémy v případě, že uživatel je členem příliš velkého počtu skupin. Problém je, že výsledná velikost tokenu při přihlášení uživatele je příliš velká a uživatelé mohou zaznamenat problémy při přihlašování, ověřování, nebo jiné problémy s protokolem Kerberos. Tento jev se často označuje jako *token bloat* (nafouknutí tokenu).

Tři různé rozsahy distribučních skupin a skupin zabezpečení souvisí s historickým odkazem na Windows NT a zavedením globálního katalogu (GC). Globální skupiny a místní skupiny domény jsou přímými potomky Windows NT skupin. Členství v těchto skupinách je k dispozici pouze na řadičích domény, ve které byly dané skupiny vytvořeny. Členství v univerzální skupině je k dispozici jak z řadiče domény, ve kterých byly dané skupiny vytvořeny, ale také na všech řadičích domény v lese, které hostují globální katalog. Univerzální a globální skupiny mohou být použity v seznamu řízení přístupu (ACL) na libovolný zdroj v lese nebo v důvěřujících doménách (doménách, mezi kterými je vytvořen trust). Místní skupiny domény mohou být použity na ACL pouze v doméně, ve které byly vytvořeny.

Následující tabulky uvádějí:

- objekty zabezpečení, které každý typ skupiny může obsahovat,
- členství ve skupině přes hranice domén.

Tabulka 2 ukazuje, které typy skupin mohou být vnořené do jiných typů skupin.

Rozsah	Typ	Může obsahovat Domain Local		Může obsahovat Domain Global		Může obsahovat Universal	
		Distribuční	Security	Distribuční	Security	Distribuční	Security
Domain Local	Distribuční	ano	ano	ano	ano	ano	ano
	Security	ano	ano	ano	ano	ano	ano
Domain Global	Distribuční	ne	ne	ano	ano	ne	ne
	Security	ne	ne	ano	ano	ne	ne
Universal	Distribuční	ne	ne	ano	ano	ano	ano
	Security	ne	ne	ano	ano	ano	ano

Tabulka 2- Členství ve skupině přes hranice domén (3)

Omezení pro všechny typy skupin jsou uvedena v tabulkách 3 a 4. Zatímco univerzální skupiny mohou obsahovat členy z různých domén, tyto domény nemohou pocházet z jiného doménového lesa. Všichni členové univerzální skupiny musí být ze stejného lesa.

Rozsah	Může obsahovat uživatele a počítače z		Může obsahovat Domain Local skupiny z	
	Místní domény	Cizí domény	Místní domény	Cizí domény
Domain Local	ano	ano	ano	ne
Domain Global	ano	ne	ne	ne
Universal	ano	ano	ne	ne

Tabulka 3- Omezení na členství ve skupinách podle rozsahu skupiny (3)

Rozsah	Může obsahovat Domain Global skupiny z		Může obsahovat Universal skupiny z	
	Místní domény	Cizí domény	Místní domény	Cizí domény
Domain Local	ano	ano	ano	ne
Domain Global	ano	ne	ne	ne
Universal	ano	ano	ano	ano

Tabulka 4- Omezení na členství ve skupině podle domény (3)

Převod skupin

Existují limity, jakým způsobem lze provádět převod skupin, a to na základě stávajících členů skupiny a současného typu a rozsahu skupiny. První z nich je dán vztahy na základě stávajících omezení uvedených v tabulce 3 – Omezení na členství ve skupinách podle rozsahu skupiny.

Proces převodu nemůže fungovat, pokud by stávající členové skupiny nemohly být členy skupiny nové.

Možnost převádět mezi skupinami má následující omezení:

- Bezpečnostní skupiny mohou být převedeny na distribuční skupiny.
- Distribuční skupiny mohou být převedeny na skupiny zabezpečení.
- Místní doménové skupiny mohou být převedeny na univerzální skupinu za předpokladu, že doménová skupina již není členem jiné doménové skupiny.
- Globální skupiny domény mohou být převedeny na univerzální skupinu za předpokladu, že globální doménová skupina neobsahuje žádné jiné globální doménové skupiny.
- Univerzální skupina může být převedena na globální doménovou skupinu za předpokladu, že všechny členy ve skupině jsou uživatelé z domény, ve které je daná skupina.
- Univerzální skupina může být převedena na místní doménovou skupinu.

Výhoda konverze distribuční skupiny na skupinu zabezpečení je zřejmá: je možné použít skupinu pro účely zabezpečení v systému Windows. Výhoda převedení bezpečnostní skupiny na distribuční skupinu není na první pohled tak zřejmá. Nejužitečnějším aspektem této konverze je fakt, že je možné převodem na distribuční skupinu bezpečně ověřit, zda je, či není používána pro účely zabezpečení v systému Windows. V starších verzích Windows, pokud nebylo jasné, zda skupina byla v minulosti použita pro účely zabezpečení systému Windows, například pokud její členové získali prostřednictvím členství v této skupině přístup k určitým souborům na souborovém serveru, jedinou možností bylo skupinu smazat a doufat, že nic nepřestalo fungovat. Pokud ale něco fungovat přestalo, bylo nutné:

- obnovit skupinu, případně přidat přístup jiné skupině. Nyní je možné jednoduše
- konvertovat skupinu na distribuční, a pokud něco přestane fungovat, je možné
- jednoduše změnit skupinu zpět na skupinu zabezpečení, čímž se funkčnost obnoví

3.2.5. Global Catalog

Globální katalog (GC) je velmi důležitou součástí Active Directory, protože se používá k vyhledání v celé doménové struktuře. Jak jeho název napovídá, Global Catalog je katalog všech objektů v lese, který obsahuje podmnožinu atributů každého objektu. GC může být

přístupné přes LDAP přes port 3268 nebo LDAP / SSL přes port 3269. Globální katalog je určen jen pro čtení a nelze ho napřímo aktualizovat.

V lesích s více doménami je zpravidla nutné nejprve provést dotaz na GC a tím daný objekt lokalizovat. Pak je teprve možné provést specifický dotaz na řadič domény, ve které je daný objekt, protože tento řadič domény na rozdíl od Globálního Katalogu již obsahuje všechny atributy objektu. Atributy, které jsou k dispozici v globálním katalogu, jsou označovány jako částečná sada atributů (Partial Attribute Set – PAS). Pomocí administrativních nástrojů, jako je například Active Directory schema snap-in, je možné v rámci PAS přidávat a odstraňovat atributy, které budou následně uloženy na všech řadičích domény Active Directory hostujících globální katalog.

3.2.6. Role hlavního operačního serveru – FSMO (Flexible Single Master Operation roles)

Přesto, že Active Directory je adresář typu multimaster, tedy všechny doménové řadiče obsahují stejná data, existují některé situace. ve kterých by měl existovat pouze jeden řadič domény, který může vykonávat určité funkce.

V těchto případech Active Directory jmenuje jeden server, který bude sloužit jako hlavní operační server (master) pro tyto funkce. Existuje pět takových funkcí, které je třeba provozovat pouze na jednom serveru.

Server, který je hlavním operačním serverem pro určitou funkci, je známý jako Flexible Single Master Operator (FSMO) nebo také vlastník role FSMO (FSMO role owner).

Z těchto pěti rolí existují tři pro každou doménu a dva se vztahují na celý les. Například v případě, že existují čtyři domény v lese, bude celkem 14 FSMO rolí:

• 2 jednotlivé role vztahující se na celý les
• 4 sady po 3 rolích vztahující se na jednotlivou doménu

Počet různých vlastníků rolí se může značně lišit v závislosti na tom, zda řadiče domény slouží pro více rolí, což je častý případ.

Různé role FSMO jsou následující: (4)

Schema master (role vztahující se na celý les)

Schema master je řadič domény, který je oprávněn provádět aktualizace schématu. Žádný jiný server nemůže provádět změny schématu. Při pokusu o aktualizaci schématu na doménovém řadiči, který není držitelem role schema master, přesměruje doménový řadič na server, který je schema master. První schema master je doménový řadič, který byl jako první povýšen na doménový řadič v rámci celého lesa.

Domain naming master (role vztahující se na celý les)

Domain naming master je server, který řídí změny v doménové struktuře názvů. Tento server přidává a odstraňuje domény a je zodpovědný za přejmenování nebo přesouvání domén v lese, také vydává povolení k založení aplikačních oddílů v Active Directory a přidání/odebrání jejich replik. Stejně jako schema master je ve výchozím nastavení tato role umístěna na serveru, který byl jako první povýšen na řadič domény v rámci celého lesa. Jedná se o běžné nedorozumění, že schema master a domain naming master nemůže být umístěn mimo kořenovou doménu. Každý řadič domény v lese (z libovolné domény) může hostovat schema master a domain naming master. Obecně se doporučuje ponechat tyto FSMO role na řadiči domény v kořenové doméně doménové struktury, pokud není vážný důvod provozovat tuto FSMO roli jinde.

PDC emulátor (role vztahující se na jednotlivou doménu)

Pro účely zpětné kompatibility se staršími systémy je nutné, aby jeden řadič domény Active Directory DC jednal jako primární řadič domény Windows NT (PDC). Tento server se chová jako Windows NT master browser, a to se také chová jako PDC pro starší klienty. Přestože PDC má velmi důležité funkce pro starší klienty, je stále velmi důležitý i v případě, že jsou ze sítě odstraněni starší klienti.

Emulátor PDC má také další důležité funkce: udržuje v databázi vždy aktuální heslo pro libovolný účet v doméně Active Directory. To je zařízeno tak, že každý další řadič domény Active Directory neprodleně předává veškeré změny hesla účtu přímo serveru PDC.

Pokud se například účet pokusí autentizovat a předkládané heslo nesouhlasí s heslem uloženým v místní databázi dotazovaného řadiče domény Active Directory. Místní DC se proto dotazuje řadiče s rolí PDC emulátor a ověřuje heslo s ním.

PDC je také primární server pro většinu nástrojů pro správu zásad skupiny (GPO). Je to proto, aby se snížila pravděpodobnost toho, že budou různí administrátoři ve stejný čas, upravovat stejnou politiku na různých řadičích domény Active Directory.

PDC je také v každé doméně primární zdroj času pro doménu a PDC kořenové domény je primární zdroj času pro celý les. PDC emulátor také opravňuje řadiče domény k operaci klonování doménových řadičů.

RID master (role vztahující se na jednotlivou doménu)

RID master existuje v každé doméně. Každý objekt zabezpečení v doméně má identifikátor zabezpečení (SID), která se skládá z několika složek včetně relativního identifikátoru – RID. Technologie Active Directory používá SID k jednoznačné identifikaci objektů pro účely zabezpečení a distribuci oprávnění. Jedná se o obdobu identifikátoru GUID, který každý objekt v AD má, ale SID je používán pouze pro zabezpečení a distribuci oprávnění. I když uživatelé používají pro ověření uživatelská jména, interně je vždy toto jméno převedeno na SID a ověřování a autorizace probíhá pomocí SID.

V jednotlivé doméně je SID jedinečný v rámci celé domény. Jelikož každý DC může vytvářet objekty, musí existovat nějaký mechanismus tak, aby nebylo možné vytvořit dva objekty se stejným SID. Aby se tomu zabránilo, RID master udržuje databázi unikátních RID hodnot. Po přidání DC do sítě je mu přidělena podmnožina 500 hodnot z RID rozsahu pro vlastní potřebu. Vždy, když DC potřebuje vytvořit SID (například administrátor vytvoří uživatelský účet v doméně Active Directory), použije další volnou hodnotu RID z vlastního rozsahu, který získal od RID mastera tak, aby vytvořil SID s jedinečnou hodnotou.

Tímto způsobem RID master zajišťuje, že všechny SID v doméně budou používat jedinečné hodnoty RID. Když doménovému řadiči klesne rozsah volných RID identifikátorů na 50 %, DC kontaktuje RID master pro další sadu RID hodnot. Tato hraniční hodnota není nastavena na 0 proto, aby bylo zajištěno, že RID master může být po krátký čas nedostupný, aniž by to mělo okamžitě dopad na možnost vytváření nových objektů. RID master sám o sobě má na starosti generování a udržování rozsahu jedinečných hodnot v celé doméně.

Velikost rozsahu RID, který si drží DC lokálně, lze nakonfigurovat pomocí nastavení RID Block Size v klíči registru HKLM \ SYSTEM \ CurrentControlSet \ Services \ NTDS \ RIDvalues na držiteli role RID master. Běžně je nutné tuto hodnotu upravit v prostředí, kde se předpokládá dlouhá doba, po kterou nebude možné kontaktovat RID master jednotlivými řadiči domény. Pokud je nutné z tohoto důvodu změnit nastavení rozsahu RID, je doporučeno změnit toto nastavení na všech doménových řadičích, které by v budoucnu potenciálně mohly nést roli RID mastera, předejde se tak nekonzistenci ve velikosti rozsahů RID pro jednotlivá DC v případě převodu role RID master na jiný DC.

Identifikátor zabezpečení (SID)

SID je jedinečný identifikátor proměnné délky, používá se k identifikaci objektů zabezpečení. SID se skládá ze dvou pevných polí a až patnácti dodatečných polí, to vše oddělené pomlčkami, třeba takto:

S-v-id-S1-S2-S3-S4-S5-S6-S7-S8-S9-S10-S11-S12-S13-S14-S15

První pevné pole (v) popisuje verzi struktury SID. V Active Directory je toto vždy 1.

Druhé pevné pole (id) se nazývá autorita identifikátoru (identifier authority). V doménách systému Windows a na Windows počítačích to jednoznačně identifikuje autentizační autoritu, hodnoty mohou být následující:

NULL (0), World (1), Local (2), NT authority (5)

Dalších 15 polí (S1-S15) není vyžadováno pro každý SID a také ve skutečnosti většina SIDů využívá jen několik málo z těchto polí. Tyto dodatečné pole se nazývají podautority (subauthorities) a pomáhají jednoznačně identifikovat odkazovaný objekt (například uživatelský účet). Poslední subauthorita se obvykle nazývá RID. To je hodnota, kterou přiřazuje SIDu doménový řadič ze svého rozsahu RIDů přidělených RID masterem. S touto informací je například zřetelné, že SID jako je S-1-5-10 znamená, že se jedná o verzi 1 SID vydané NT autoritou. Tento SID je navíc zvláštní a je nazýván známý SID, což představuje NT AUTHORITY\Self. Další dobře známý SID je S-1-1-0, což je verze 1 = World SID, který znamená Everyone – neautentizovaný uživatel.

Existuje několik dalších známých identifikátorů s různými hodnotami. Jsou snadno identifikovatelné, protože nezapadají do formátu běžných počítačových a doménových SID identifikátorů. Tyto SIDy obvykle vypadají například takto: S-1.5.21-xxx-yyy-zzz-r, kde hodnoty xxx, yyy a zzz jsou generovány náhodně, když je vytvořen počítač nebo doména. Hodnota r – RID může být buď pořadové číslo vydané RID masterem nebo dobře známý RID (well known RID), přiřazeny k určitým objektům, které existují v každé doméně. Příklad dobře známého RID je 500, což znamená vestavěný účet správce. Tento účet má nejvyšší oprávnění v doméně, a proto je často cílem útoků hackerů.

Hlavní server infrastruktury (*Infrastructure master,* role vztahující se na jednotlivou doménu) Infrastructure master se používá k udržení odkazů na objekty v jiných doménách, tzv. Phantom objects. Pokud tři uživatelé z domény B jsou členy skupiny v doméně A, Infrastructure master se používá k udržení reference na phantom objekty uživatelů domény B. Tyto phantom objekty nejsou spravovatelné nebo viditelný přes běžné nástroje správy Active Directory, ale jsou pouze implementací technologie k udržení konzistence. (5)

Infrastructure master neustále udržuje informace o phantom objektech z jiných domén, když objekty, na které phantom objekty odkazují, jsou ve své doméně přesunuty nebo změněny, infrastructure master opraví tuto informaci na phantom objektu. Držitel role Infrastructure master je zodpovědný za aktualizaci SID a Distinguished Name atributů v odkazu na objekt v jiné doméně.

Infrastructure master je také zodpovědný za opravu neplatných referencí na objekty v jiných doménách. Děje se tak na základě porovnání jeho informací s informacemi, které jsou v Global Catalogu, který automaticky přijímá pravidelné aktualizace pro objekty ve všech doménách v lese, a tudíž nemá zastaralá data. Infrastructure master zapisuje všechny nalezené změny na své objekty a poté replikuje aktualizované údaje na ostatní řadiče domény Active Directory. V případě, že držitel role infrastructure master je zároveň Global Catalog server, z principu funkce serveru Global Catalog to znamená, že bude mít vždy aktuální data a nebude tedy mít žádné staré reference, které by bylo potřeba aktualizovat. Z této vlastnosti plyne jistá nevýhoda umístění této role na server Global Catalog. Pokud je Global Catalog zároveň infrastructure master, tím, že má vždy aktuální data z Global Catalogu, se nikdy nedozví o případných změnách, které by za normálních okolností replikoval na doménové řadiče, na kterých není Global Catalog. Z toho plyne doporučení neumísťovat roli Infrastructure Master na DC, který

je zároveň i Global Catalog, nebo umístit Global Catalog na všechny doménové řadiče tak, aby byla zajištěna konzistence dat. (6)

Jakmile je v Active Directory aktivována funkce AD Recycle Bin, funkce infrastructure mastera jsou prováděny nezávisle na této roli na každém z DC v lese a nejsou již prováděny pouze jedním serverem.

Infrastructure master je navíc zodpovědný za provádění aktualizací na doménách při upgradu na systém Windows Server 2003 nebo novější – příkaz adprep / domainprep musí být spuštěn na Infrastructure masteru.

Umístění role infrastructure master a to, zda může nebo nemůže být umístěn na DC, který je zároveň i globální katalog, aniž by to způsobilo problémy, je často zdrojem velkého zmatku. Následující tabulka poskytuje matici povolených možností pro lesy Active Directory. Recycle Bin není povolen.

	Forest s jednou doménou	Forest s více doménami	
		Všechny DC jsou GC	Všechny DC nejsou GC
Infrastructure master role musí být zohledněna	Ne	Ne	Ano
Infrastructure master může být na GC	Ano	Ano	Ne

Tabulka 5- Matice povolených možností Globálního Katalogu pro lesy Active Directory (1)

Role FSMO lze přenášet mezi řadiči domény. Domain naming master roli je možné převést pomocí Active Directory domains and trusts mmc snapinu. Schema master roli je možné převést pomocí schema management modulu snap-in. a dále RID-master.

Infrastructure master a PDC emulater role je možné převést pomocí Active Directory Users and Computers snap-inu. Případně je možné použít nástroj ntdsutil k provádění převodů z příkazového řádku.

Ačkoli AD snap-in a NTDSUTIL může jednoduše přenést roli FSMO z jednoho serveru na druhou v případě, že oba servery jsou k dispozici, může se vyskytnout scénář, ve kterém vlastník role FSMO není k dispozici, aniž by roli dříve převedl – například z důvodu nenadálého výpadku serveru. V tomto případě, bude potřeba použít NTDSUTIL a vynutit přenos role na jiný server. Tato procedura je známá jako "seize" FSMO role. Pokud je nutné použít tuto proceduru násilného převzetí role FSMO, původní majitel této role by se nikdy

neměl vrátit zpět do online režimu. Místo toho by mělo být provedeno vyčištění metadat a původního řadiče domény a nový řadič domény by měl být nainstalován.

Ve verzi Windows Server 2008 nebo novější konzole Active Directory users and computers umožňuje odstranit řadiče domény přímo z této konzole a vyčištění metadat bude provedeno automaticky bez nutnosti použít nástroj příkazové řádky NTDSUTIL. Pro dřívější verze je nutné použít nástroj NTDSUTIL z příkazové řádky.

Pokud dojde ke ztrátě jednoho z držitelů role FSMO, je nutné tuto situaci co nejrychleji napravit – buď zprovozněním serveru, který je držitelem patřičné role, nebo násilně převést (seize) tuto roli na jiný řadič domény. Pokud server s rolí není k dispozici, jiný server se automaticky nepostará o převzetí role. Správce to musí udělat ručně.

Dopady nedostupnosti jednotlivých rolí FSMO

Schema master

Schema master je nutný pouze tehdy, pokud se provádí změny schématu. Ty jsou obvykle plánovány v dostatečném předstihu, takže pokud se schema master stane nedostupným, nemá to dopad na provoz domény.

Domain naming master

Domain naming master je potřebný pouze při přidávání domén a aplikačních partícií do Active Directory. To je další změna, která je plánována s dostatečným předstihem, takže nedostupnost serveru s touto rolí opět nemá dopad na provoz domény.

Infrastructure master

Je-li infrastructure master nedostupný, nelze spustit příkaz adprep /domainprep a zastaví se aktualizace phantom objektů z cizích domén. Infrastructure master aktualizuje phantom objekty v intervalu několika dní, takže existuje velká šance, že než dojde k jeho navrácení do provozu, nebude funkčnost aktualizace nijak omezena. Pokud je povolen Active Directory Recycle Bin, výpadek řadiče domény s rolí infrastructure master bude mít vliv pouze na schopnost spouštět příkaz adprep. (4)

RID master

V případě, že RID master je offline, nelze vydávat rozsahy RID všem ostatním DC v doméně. Řadiče domény žádají o RIDy v blocích po 500, když se dostanou až na 250 zbývajících, požádají RID master o dalších 500 RIDů. Pokud tedy nedojde k vytvoření velkého počtu objektů během doby nedostupnosti RID mastera, nedojde k žádnému omezení provozu služby Active Directory, pokud ale dojde k vytvoření velkého množství objektů – více objektů, než kolik volných RIDů zbývalo ve fondu na patřičném DC, dojde po vyčerpání tohoto rozsahu k chybě a nebude možné dále vytvářet nové objekty. Další funkčnost AD to ale neovlivní, autentizace a autorizace bude fungovat dále.

PDC emulátor

Význam dostupnosti PDC emulátoru se liší prostředí od prostředí. Emulátor PDC je řadič domény, který využívají aplikace, které používají starší rozhraní API. Také ale hraje klíčovou roli ve vztazích důvěry (Trust) s dalšími doménami, je důležitý při změně hesla, je to autoritativní zdroj času pro doménové řadiče a tak dále. Dopad nefunkčnosti PDC emulátoru může být různý, ale obecně je možné prohlásit, že z pěti FSMO rolí je PDC emulátor pravděpodobně nejdůležitější držitel role ve vašem prostředí.

3.3 Single Sign-On

Běžně užívaná zkratka SSO (Single Sign-On), neboli jednotné přihlašování, popisuje metodu, kdy uživatel zadá své přihlašovací údaje jen jednou na začátku, tyto údaje jsou následně ověřeny centrální ověřovací autoritou. Následně při pokusu o přístup k nějakému zdroji (soubor, intranet, webová stránka) dojde k přihlášení bez nutnosti zadávání přihlašovacích údajů. Toto řešení je nejen pohodlné pro uživatele, protože nemusí neustále zadávat své přihlašovací údaje, ale je to také bezpečnější; přihlašovací údaje totiž uživatel nikdy nezadává službě, ke které chce získat přístup, ale pouze autentizační autoritě, která potom předá službě důvěryhodnou informaci o tom, že uživatel byl ověřen, a ten na tomto základě získá přístup k dané službě.

3.3.1. Protokol Kerberos

Jednou z nejdůležitějších technologií, na kterých je založena Active Directory, je bezpečnostní protokol Kerberos. Kerberos poskytuje ověřovací mechanismus, který umožňuje přihlášení uživatele, přístup k aplikacím a komunikaci mezi řadiči domény. Implementace technologie

Kerberos je možná i bez produktu Active Directory, avšak jedná se o komplexní a náročný úkol, sám protokol Kerberos zahrnuje množství komponent, které je nutné zvlášť nakonfigurovat. Naproti tomu po instalaci Active Directory není nutná žádná další konfigurace pro to, aby bylo možné používat Kerberos.

Klíčovým přínosem bezpečnostního protokolu Kerberos je umožnit uživateli bezpečně prokázat svou identitu a potom využít jednotného přihlášení k dalším službám. Ve skutečnosti s protokolem Kerberos hesla nejsou nikdy přenášena přes síť ve formátu prostého textu nebo i šifrovaně. Namísto toho jsou generovány klíče specifické pro danou relaci a jsou platné jen velmi krátkou dobu. (7)

Přihlášení uživatele

Předmětem zájmu je uživatelské přihlášení k počítači potom, co uživatel zapne počítač a stiskne Ctrl-Alt-Delete.

Klíčem k jednotnému přihlášení s použitím protokolu Kerberos je první krok v procesu přihlašování: získání ticket granting ticket (TGT). Když se uživatel přihlásí na pracovní stanici, Windows ukládá TGT a používá ho k získání ticket granting service (TGS), aniž by bylo nutné vyzvat uživatele znovu k zadání hesla, když chce získat přístup ke službě v síti.

Prvním krokem v procesu ověřování je, že klient si vyžádá předběžné ověření v paketu AS_REQ (authentication service request). Obrázek 4 ukazuje obsah AS_REQ zprávy. AS_REQ obsahuje potřebné informace k prokázání identity uživatele doménovému řadiči.

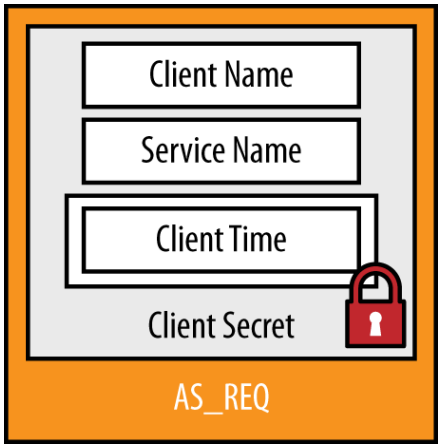
Tyto údaje jsou následující:

Client Name – odpovídá uživatelskému jménu

Service Name – je service principal name (SPN) služby KRBTGT na řadiči domény.

Client Time – systémový čas na počítači uživatele – k prokázání identity uživatele je aktuální čas na straně klienta zašifrován pomocí hashe (kontrolního součtu) hesla uživatele. Řadič domény se pokusí dešifrovat toto pole použitím hashe hesla uloženého v databázi služby Active Directory. Časové razítko je poté kontrolováno, jestli je v rámci tolerance odchylky času (+/- pět minut, ve výchozím nastavení), aby se zabránilo tzv. replay útokům (hacker nahraje provoz

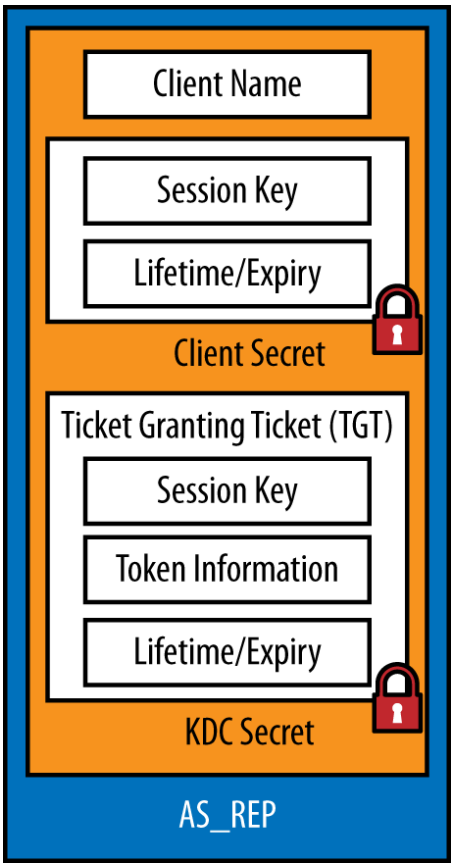
na síti obsahující kerberos tickety, a pokusí se je „přehrát“ znovu na doménovém řadiči, aby získal autentizaci).



Obrázek 4- Paket pro autentizační službu (2)

V případě, že uživatel používá přihlášení pomocí čipové karty namísto uživatelského jména a hesla, následuje poněkud odlišný proces šifrování. Místo zašifrování časové hodnoty pomocí hashe hesla uživatele je časová hodnota zašifrována pomocí soukromého klíče uživatele (uloženého na čipové kartě). DC použije veřejný klíč uživatele (uložený v AD) za účelem ověření platnosti podpisu na žádosti, a tím ověří uživatele. Jakmile DC validuje požadavek na ověření, je možné vydat TGT. (5)

Samotný TGT je zapouzdřen v AS_REP (autentication service reply) paketu, jak je znázorněno na následujícím obrázku. TGT obsahuje přístupový token (access token) uživatele a kopii klíče relace (session key), který se používá pro komunikaci mezi klientem a DC v budoucnu.



Obrázek 5- Paket s odpovědí od autentizační služby (2)

Paket s odpovědí od autentizační služby – Obrázek 5

Pole ve zprávě AS_REP jsou následující:

Client Name – odpovídá uživatelskému jménu

Session Key – klíč relace – jedná se o náhodný kryptografický klíč, který se používá k zabezpečení další komunikace mezi řadiči domény a klientem. Klíč relace je zašifrován pomocí hashe uživatelova hesla.

Lifetime/Expiry = TGT tikety mají definovanou dobu životnosti (10 hodin ve výchozím nastavení). Po 10 hodinách musí být tikety TGT obnoveny nebo musí být podán nový požadavek na ověření. Toto pole je šifrováno hashem hesla uživatele. (5)

Ticket Granting Ticket – TGT je součást, kterou bude klient následně udržovat v paměti a používat jí pro žádání o servisní tikety, takzvané TGS (ticket granting service). Celý TGT tiket je zašifrován pomocí hashe služby KDC (Key Distribution Center) - tedy hashem hesla účtu KRBTGT, pod kterým daná služba běží. To znamená, že obsah TGT není pro klienta

známý, protože klient nezná heslo účtu KRBTGT, toto heslo je známé pouze pro účet doménového řadiče.

Uvnitř TGT je uložena kopie session key, aby DC mohl dešifrovat budoucí komunikaci s klientem, dále je zde uložena informace o době použitelnosti tiketu. Co je nejdůležitější, access token uživatele je také uložen v TGT. Access token obsahuje důležité informace, jako je členství ve skupinách, uživatelova práva a také Dynamic Access Control (DAC) Claimy uživatele.

Jakmile klient obdrží AS_REP zprávu, klient nejprve dešifruje klíč relace a ukládá jej do paměti vedle TGT. V tomto okamžiku heslo uživatele již není nezbytné, protože všechna budoucí Kerberos komunikace s DC bude chráněna použitím klíče session key.

Přístup ke službám

Jakmile uživatel získá tiket TGT, může začít přistupovat ke službám využívající Kerberos. TGT získaný v předchozím kroku je důkazem, že uživatel byl již ověřen pomocí DC, a tedy není nutné, aby uživatel zadával znovu uživatelské jméno a heslo a byl znovu ověřován.

Kerberos mohou využívat prakticky všechny síťové služby. Typicky se jedná o služby jako souborové a tiskové servery, webové stránky, databáze, limit je pouze schopnost aplikace přijmout autentizaci pomocí Kerberos. Klienti identifikují službu, ke které chtějí získat přístup, pomocí service principal name (SPN). (6)

Service principal names

Podobně jako jsou uživatelé identifikováni v adresáři unikátním jménem UPN (Unique Principle Name), služby jsou identifikovány jedním nebo více jmény SPN (Service Principle Name). SPN jsou identifikátory, které klienti využívají, když požadují servisní tiket od DC pro danou službu.

SPN je vytvořeno jako identifikátor služby, po němž následuje Hostname - např. služba/hostitel. Identifikátor služby je předdefinovaný řetězec, který musí být známý jak klientovi, tak serveru, např. služby sdílení souborů jsou přístupné pomocí názvu služby CIFS.

Název hostitele může být buď jméno serveru nebo služby, nebo také plně kvalifikované doménové jméno (FQDN – fully qualified domain name) serveru nebo služby na něm běžící. Často jsou registrovány oba názvy, jak krátký, tak FQDN.

Například webový server s názvem WEB01.czu.cz může mít následující SPN registrované v Active Directory:

• http / WEB01
• http / WEB01.czu.cz

SPN mohou také volitelně obsahovat číslo portu.Microsoft SQL

Server je příkladem produktu, který přidává port do SPN názvu. SQL Server s názvem DB01.czu.cz tak bude mít následující SPN registrované ve službě Active Directory:

• MSSQLSvc / DB01: 1433
• MSSQLSvc / DB01.czu.cz: 1433

Název služby a hostname jsou v podstatě libovolné části SPN. Jediné, co musí být splněno je, že v klientově žádosti o vydání TGS musí být uvedeno SPN stejné jako SPN služby.

SPN jména jsou uložena v Active Directory v servicePrincipalName atributu. Tento atribut může mít více hodnot. To znamená, že jedna služba může mít více SPN. AD objekty uživatel, počítač a service managed account mohou mít vyplněn servicePrincipalName atribut. SPN služby musí být uloženo v atributu servicePrincipalName účtu, pod kterým je služba spuštěna. Pokud je aplikace spuštěna pod standardním uživatelem nebo spravovaným účtem, SPN názvy by měly být registrovány na daný objekt. Pokud je aplikace spuštěna jako LOCAL SYSTEM nebo NETWORK SERVICE, SPN názvy by měly být registrovány na objekt počítače, na kterém služba běží. (3)

SPN názvy mohou být nastaveny pomocí nástroje jako například ADSIEdit nebo Attribute Editor v konzoli dsa pouhým přidáním atributu servicePrincipalName. Také lze použít nástroj příkazového řádku setspn.exe. (6)

Výhodou Setspn.exe je, že lze provádět vyhledávání duplicitních záznamů před samotnou registrací SPN. Například při registraci SPN SQL Serveru diskutovaném dříve – Server DB01,

kde běží SQL Server pod uživatelským účtem svc.DB 01SQL, bude třeba spustit následující příkazy:

setspn -s MSSQLSvc / DB01: 1433 svc.DB01SQL
setspn -s MSSQLSvc / DB01.czu.cz: 1433 svc.DB01SQL

Servisní tikety

Pokud se uživatel rozhodne pro přístup ke službě, napřed je sestaven požadavek v paketu TGS_REQ (ticket granting service request). TGS_REQ obsahuje pole zobrazené na následujícím obrázku. Tyto údaje jsou:

Service Principal

To je SPN, který jednoznačně identifikuje službu, na kterou se uživatel pokouší připojit.

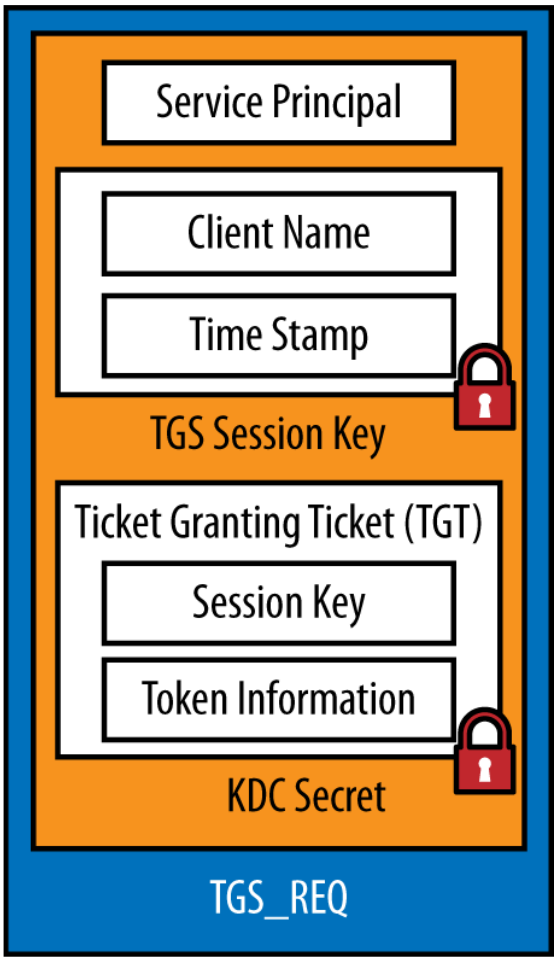
Client Name – odpovídá uživatelskému jménu, je zašifrováno pomocí session key, který byl vygenerován během procesu ověřování.

Časová známka

Toto pole zabraňuje útokům pomocí přehrání tím, že zajistí, aby žádost nebylo možné znovu použít více než dlouhou dobu. Ve výchozím nastavení je požadavek platný pouze pro +/- pět minut. Toto pole je také zašifrováno pomocí session key.

TGT

Kopie TGT je zahrnuta v žádosti. DC používá TGT pro vytvoření TGS a také pro ověření, že je uživatel ověřen a platnost TGT nevypršela.



Obrázek 6- Paket žádosti o tiket TGS (2)

Pokud doménový řadič obdrží TGS_REQ zprávu, nejdříve se pokusí najít službu, která má stejné SPN jako SPN služby v žádosti. Tento proces má dva kroky – za prvé proběhne standardní hledání, jestli existuje explicitní SPN záznam. Pokud není možné najít explicitní SPN záznam, služba se pokusí najít implicitní SPN záznam. Každý účet, který má jeden nebo více explicitních SPN ve formátu HOST/Služba (např. HOST / SRV01.czu.cz) automaticky přijímá několik desítek dalších SPN prostřednictvím procesu implicitního přiřazení SPN. Účelem tohoto procesu je omezit množství duplikovaných dat. Kdyby tento proces neexistoval, bylo by nutné replikovat každý implicitní SPN zvlášť. Tyto SPN popisuje následující tabulka.

Seznam implicitně mapovaných SPN je možné upravit pomocí sPNMappings atributu na objektu CN=Directory Service, CN = Windows NT, CN = Services objektu. Je možné přidat další implicitní mapování pro název hostitele služby nebo přidat implicitní mapování s jiným názvem služby. (7)

Existuje několik možných výsledků procesu vyhledávání SPN:

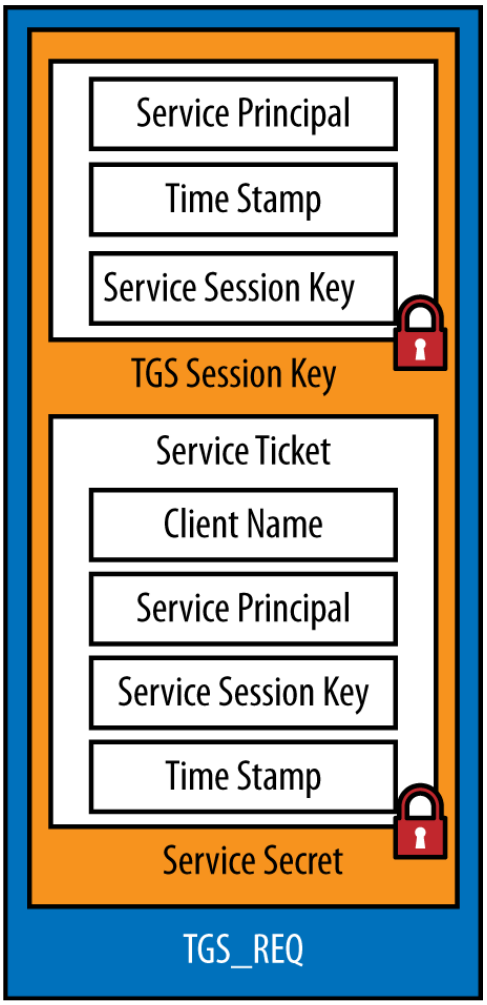
- Je nalezena shoda a service ticket může být vydán.
- Je nalezeno více shod (duplicitní servicePrincipalName hodnoty atributů ve forestu). V tomto případě je vrácena chyba, protože Active Directory neví, které SPN má použít.
- SPN v databázi AD neodpovídá SPN v žádosti, shoda není nalezena, a tedy je vrácena chyba.

Výchozí seznam SPN, které jsou implicitně namapovány na hostitele, je uveden v následující tabulce:

alerter	fax	plugplay	schedule
appmgmt	http	policyagent	scm
browser	ias	protectedstorage	seclogon
cifs	iisadmin	rasman	snmp
cisvc	messenger	remoteaccess	spooler
clipsrv	msiserver	replicator	tapisrv
dcom	mcsvc	rpc	time
dhcp	netdde	rpclocator	trksvr
dmserver	netddedsm	rpcss	trkwks
DNS	netlogon	rsvp	ups
dnscache	netman	samss	w3svc
eventlog	nmagent	scardsvr	wins
eventsystem	oakley	scesrv	www

Tabulka 6- Seznam implicitních SPN

Za předpokladu, že služba nalezne shodu s SPN v žádosti TGS_REQ doménový řadič, zkontroluje TGT (například jestli nevypršel – replay útok popsaný výše) a postoupí dále k vydání servisního tiketu pro danou službu. Tento tiket je následně vydán pomocí TGS_REP (Ticket Granting Service – Reply) paketu, jenž je znázorněn na dalším obrázku.



Obrázek 7- Paket s odpovědí od TGS služby (2)

TGS_REP má následující části:

Service Principal

Jedná se o SPN služby, pro kterou platí daný service ticket. Toto pole je zašifrováno pomocí session key, který byl zřízen dříve v průběhu ověřovacího procesu.

Time Stamp

Časové razítko zprávy, které se používá k zabránění proti replay útokům. Toto pole je také zašifrováno pomocí session key, který byl zřízen dříve v průběhu ověřovacího procesu.

Service Session Key

Jedná se o druhý klíč, který je v mezipaměti klienta pro šifrování komunikace s konkrétní službou. Toto pole je také zašifrováno pomocí session key, který byl zřízen dříve v průběhu ověřovacího procesu.

Servisní tiket

Tento servisní tiket je to, co bude klient prezentovat službě při žádosti o přístup. Tento servisní tiket zároveň klient ukládá do paměti pro pozdější přístup ke službě. Podobně jako TGT je servisní tiket nečitelný klientovi; je šifrován pomocí hashe hesla služby, ke které se pokouší klient přistoupit.

Servisní tiket obsahuje jméno klienta, SPN služby, kopii service session klíče, který bude klient používat k šifrování komunikace se službou, a časové razítko. Uvnitř servisního tiketu je kopie access tokenu, který byl vydán při původní žádosti klienta o TGT (TGT_REQ). Služba může použít tyto informace (jako například členství ve skupině) k autorizaci přístupu uživatele ke službě. Stejně jako TGT, obsahuje servisní tiket datum vypršení platnosti a po uplynutí této doby bude servisní tiket obnoven.

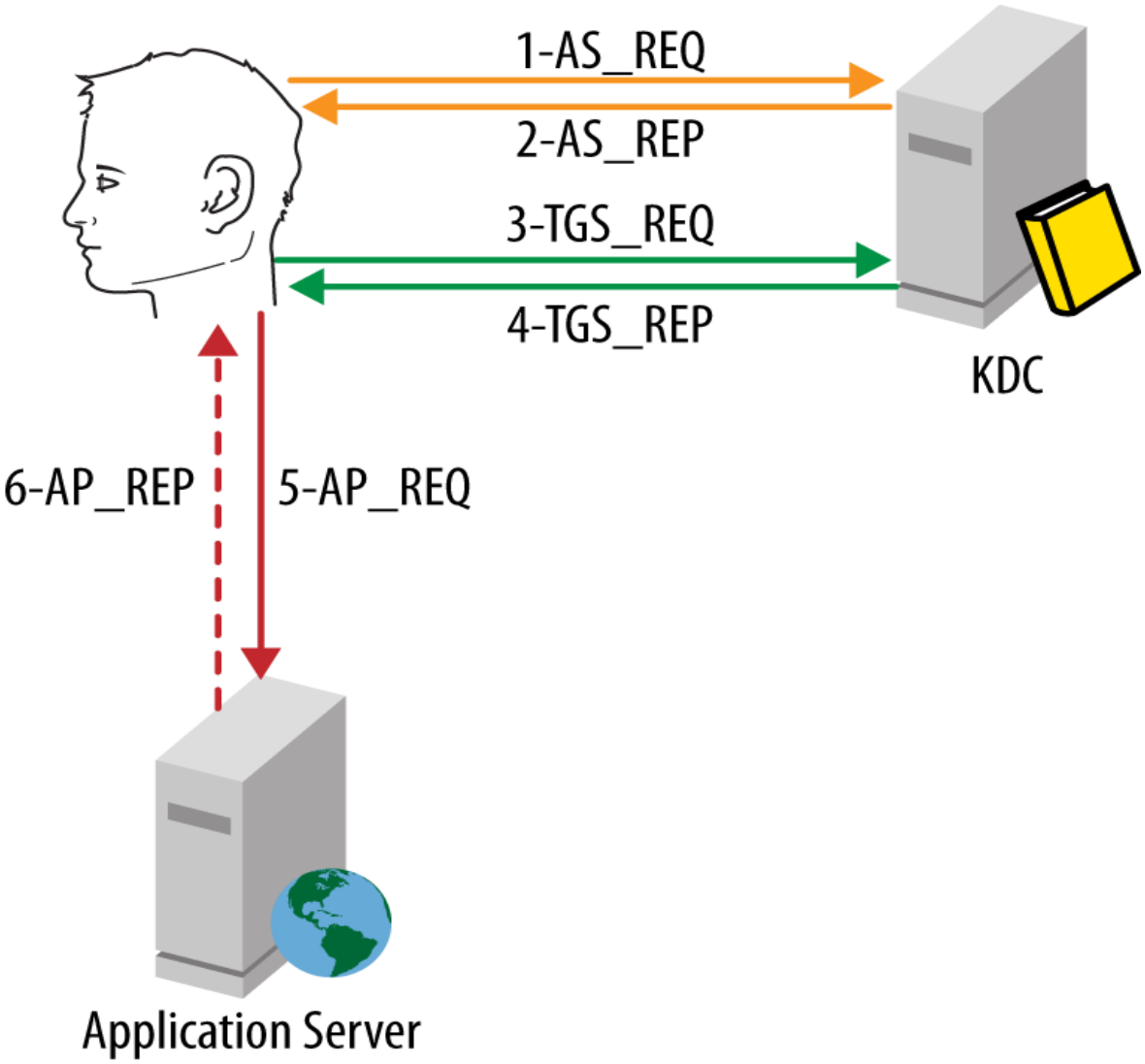
Přístup k aplikaci

Jakmile má klient servisní tiket pro službu, předloží tento tiket při požadavku na přístup k této službě. Servisní tiket je presentován službě jako AP_REQ zpráva. Na rozdíl od zpráv zmiňovaných doposud, AP_REQ zprávy jsou prezentovány jiným způsobem pro každou aplikaci. Například pro webové aplikace je zpráva zakódována v HTTP záhlaví, zatímco v případě protokolu LDAP je součástí žádosti o spojení.

Aplikace mohou také volitelně podporovat vzájemné ověřování (přičemž služba také prokazuje svou identitu zpět klientovi) za použití AP_REP zpráv.

Shrnutí procesů přihlášení a přístupu ke službám:

Následující obrázek shrnuje proces zmiňovaný výše:



Obrázek 8- Souhrn toku zpráv protokolu Kerberos (4)

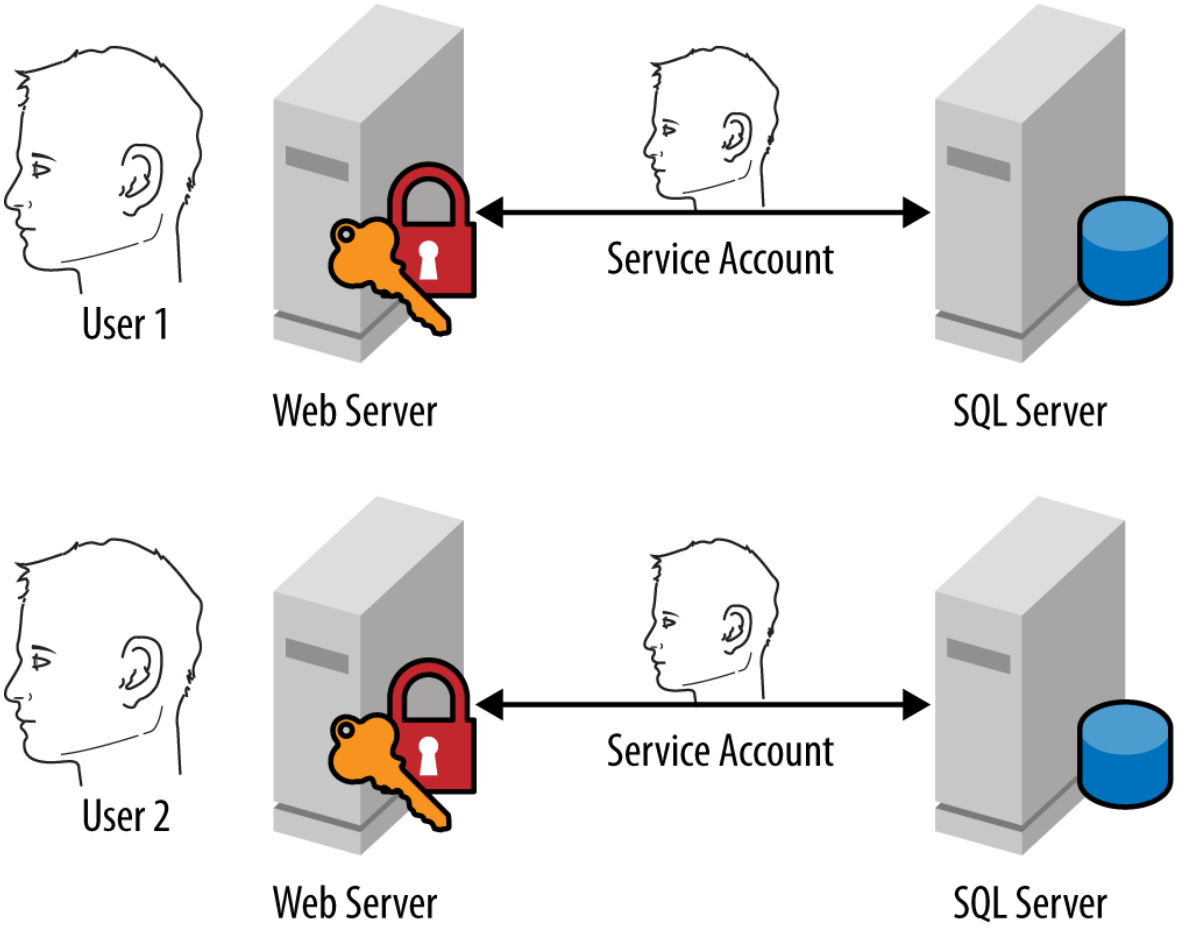
Při pohledu na tento proces je patrné, že Kerberos umožňuje jak jednotné přihlášení, tak vyšší stupeň bezpečnosti. Vzhledem k tomu, že je TGT uložený v paměti na straně klienta, uživatelovo heslo již není nutné znovu zadávat. V průběhu životnosti tiketu TGT jej může klient předkládat řadiči domény mnohokrát, pokaždé když žádá o servisní tiket pro konkrétní službu v síti. Tyto servisní tikety jsou pak uložené v paměti na straně klienta a jsou předloženy službám kdykoliv klient potřebuje ověření. (6)

Kerberos constrained delegation (KCD)

Jednou z funkcí protokolu Kerberos, která je často využívána, zejména v případě webových aplikací s databází, se nazývá Kerberos constrained delegation (KCD). KCD umožňuje aplikaci jednat jménem uživatele a podat žádost na jinou službu jeho jménem.

Delegace

Existuje několik běžných modelů, které aplikace používají, když potřebují, aby mohla číst (nebo modifikovat) data z jiného systému. První model je známý jako trusted subsystem, jak je znázorněno na následujícím obrázku. V tomto modelu se uživatel autentizuje do aplikace (webový server v tomto případě) a následně ke všem datům přistupuje pomocí servisního účtu aplikace.



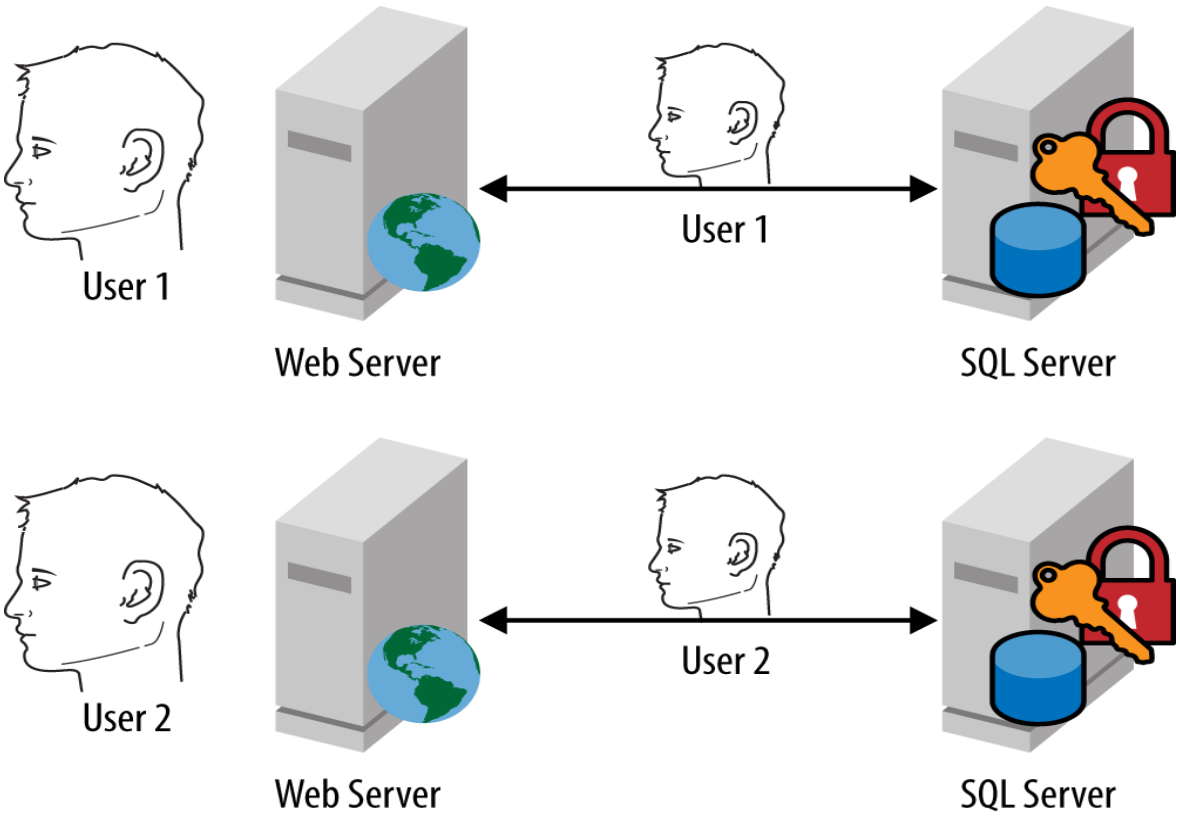
Obrázek 9- Model trusted subsystem (2)

Nevýhodou tohoto modelu je, že aplikace je zodpovědná za implementaci modelu autorizace.

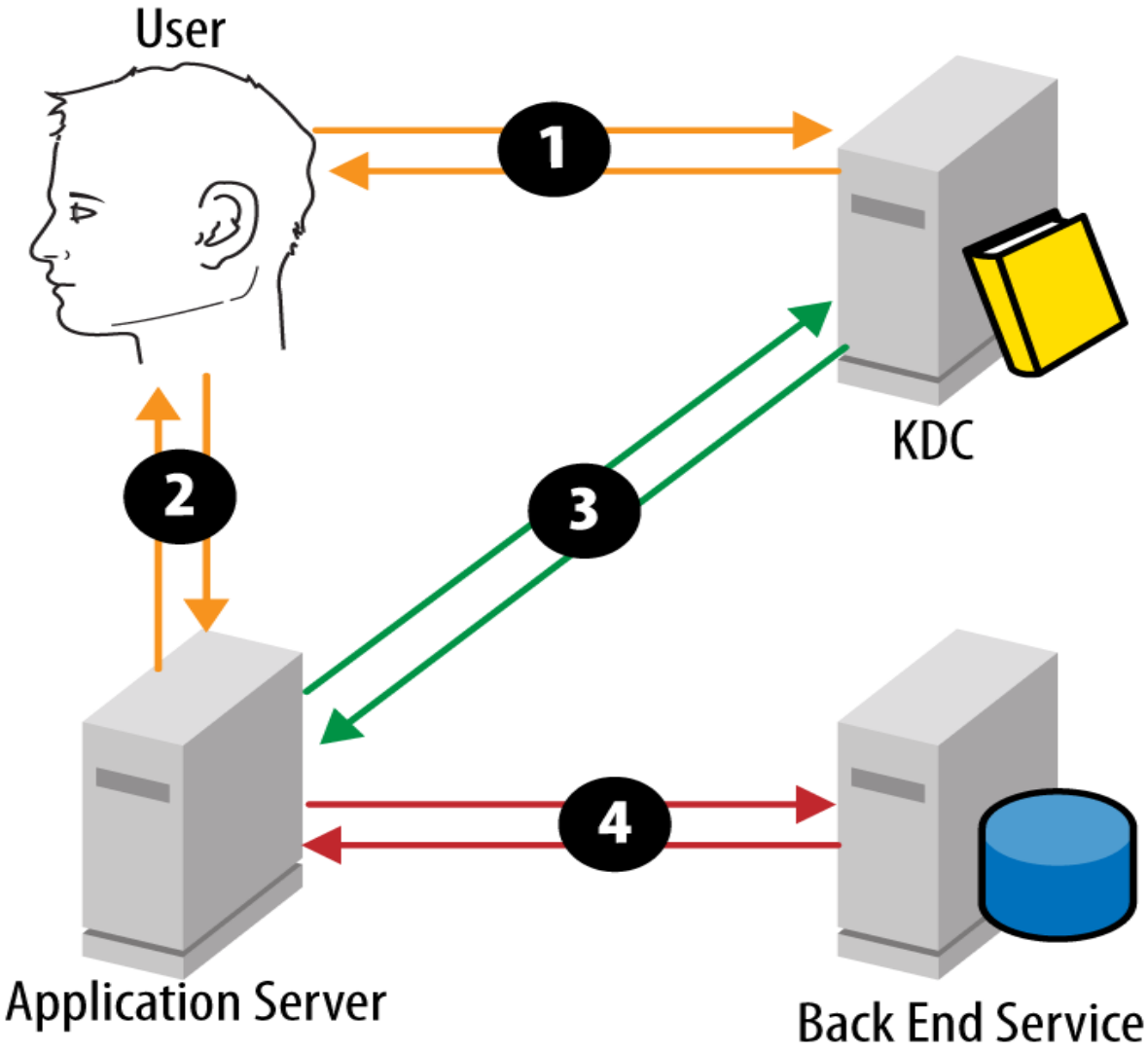
Alternativou je model, kdy je autorizace přenechána backend systému, v tomto případě SQL serveru. SQL server provede autorizaci a jednoduše vrátí pouze ta data, ke kterým má uživatel přístup, tak jak je znázorněno na následujícím obrázku. Za účelem dosažení tohoto cíle se webový server musí vydávat za každého uživatele pokaždé, když se připojí k backend SQL serveru.

Aby toto bylo možné, webový server potřebuje mít možnost požádat o servisní tiket pro službu SQL serveru pro každého uživatele. Následující kroky provádí webový server při žádosti o servisní tiket:

1. Uživatel požádá o servisní tiket na frontendové službě – v tomto případě web server.
2. Uživatel se frontend serveru prezentuje tiketem TGT.
3. Frontend server následně přepošle TGT tiket na DC a vyžádá si servisní tiket pro službu SQL serveru
4. Frontend serveru odešle servis tiket na backend službu a dále jedná s touto službou jménem uživatele.



Obrázek 10- Delegovaný přístup k backend serveru (2)

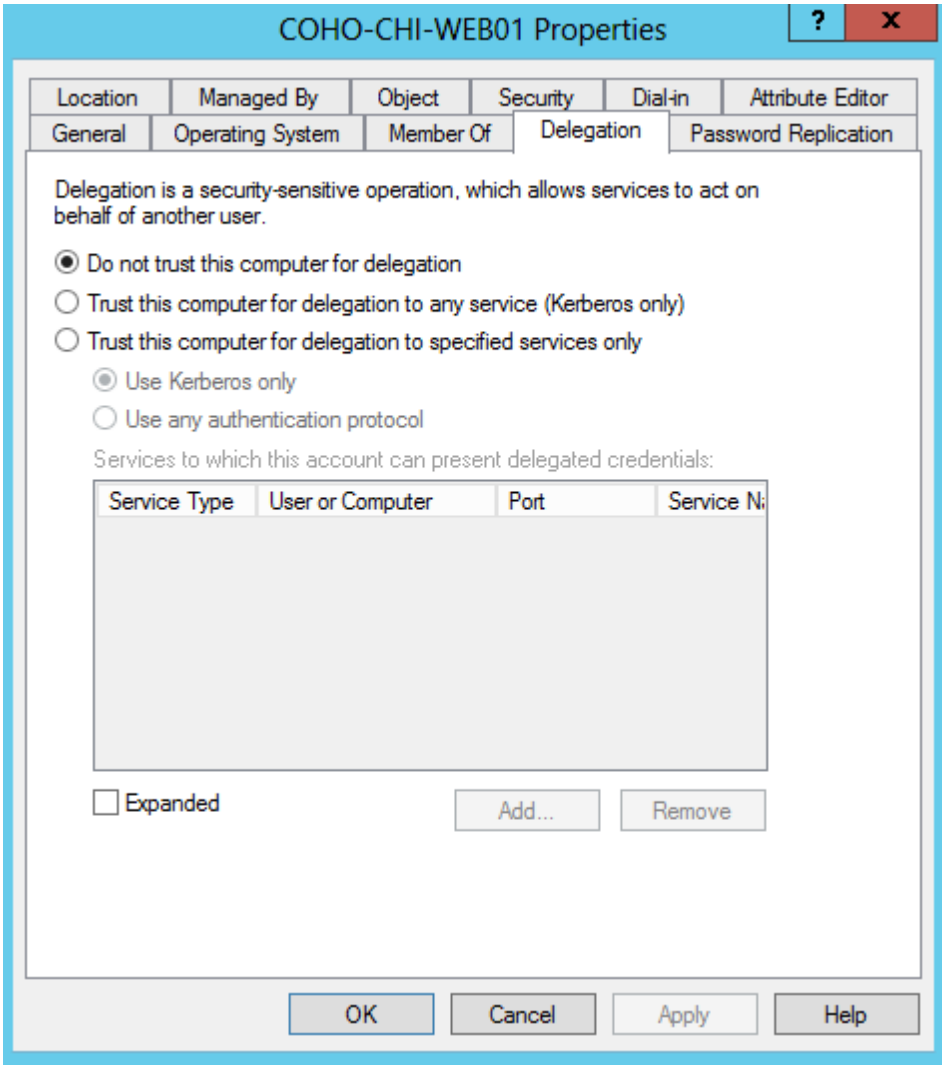


Obrázek 11- Tok kerberos zpráv během delegace (2)

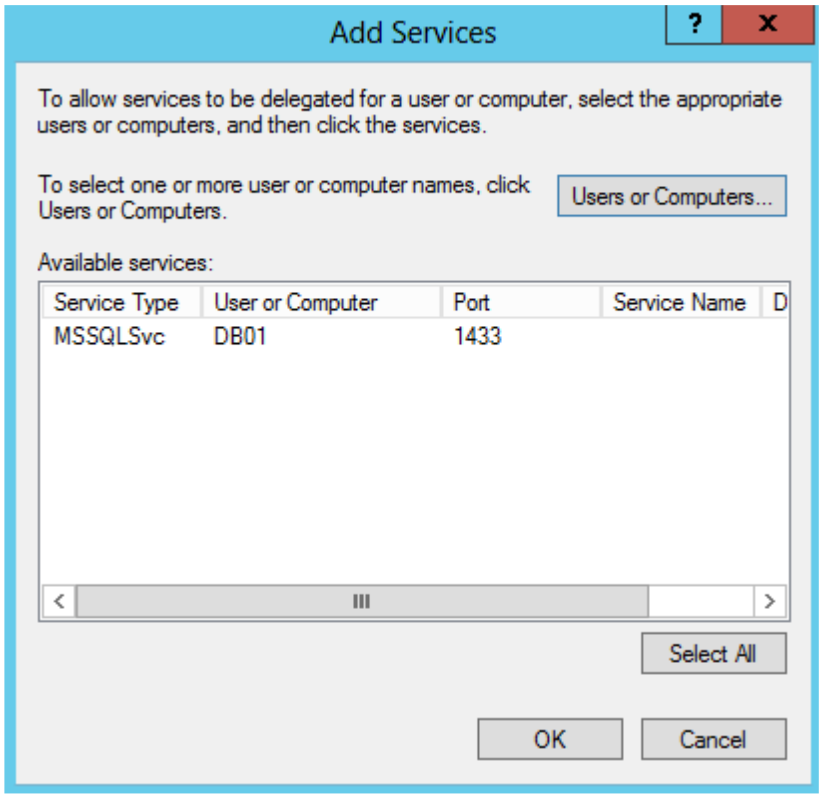
Tento proces je známý jako delegace. Vzhledem k tomu, že další službě je uděleno právo zosobnit uživatele a přistupovat jeho jménem k další službě, jedná se o velmi citlivou operaci. V důsledku toho služby nemohou jednoduše tuto operaci provést bez povolení.

Povolení se uděluje v Active Directory ve formě explicitního povolení možnosti přenést ověření na jinou službu. Toto je známé jako constrained delegation. Nejjednodušší způsob, jak nakonfigurovat constrained delegation je přes kartu delegation ve snap-inu Active Directory users and computers, jež je součástí nástrojů pro správu Active Directory.

Delegace je nakonfigurována na účtu frontendové služby jakožto povolení delegovat na jedno nebo více SPN. Jedná se o účet služby, pokud je služba spuštěna jako daný účet, a účet počítače v případě, že služba je spuštěna jako LOCAL SYSTEM nebo NETWORK SERVICE.



Obrázek 12- Karta Delegation



Obrázek 13- Karta delegation – přidání služby

To je vše, co je nutné k tomu, aby server COHO-CHI-WEB01 mohl přistupovat jménem uživatele na službu MSSQLSvc / DB01.czu.cz: 1433 SPN.

Pokud je systém založen nad systémem Windows Server 2012 a splňuje následující požadavky, je možné také nastavit delegování pomocí prostředí Windows PowerShell:

- Frontend služba je spuštěna na systému Windows Server 2012 nebo Windows 8.
- Backend služba běží na Windows Server 2003 nebo novější.
- Alespoň jeden řadič domény Windows Server 2012 existuje v doméně, kde je frontend služba
- Alespoň jeden řadič domény Windows Server 2012 existuje v doméně, kde je backend služba

Tento model také umožňuje KCD přes hranice domén. Dříve KCD mohl být proveden, jen když oba frontend a backend byly umístěny ve stejné doméně.

3.4 Active Directory v moderním IT

Technologie Active Directory byla navržena v době, kdy uživatelé používali pracovní stolní počítač nebo nanejvýš přenosný laptop. Data byla uložena na serveru, který byl přístupný pouze z vnitřní sítě. Uživatelé pracovali hlavně z kanceláře. Následně s rozvojem internetu a tím, jak se internetová konektivita stávala čím dál dostupnější, bylo možné některým uživatelům umožnit připojení do firemní sítě i z domova pomocí VPN sítě, princip autentizace ale zůstal stále stejný; uživatel se autentizoval prostřednictvím Active Directory ke zdroji ve vnitřní síti, ke kterému se chystal přistoupit. Tento způsob vydržel další desetiletí a v mnoha společnostech funguje dodnes.

S dalším rozvojem technologií, zvyšováním výkonu, zrychlováním internetu a zvyšování jeho dostupnosti přišel i fenomén cloudových služeb. Cloudové služby jsou dostupné přes internet, snadno rozšiřitelné, placené na bázi použití. Mnoho společností začalo využívat služeb v prostředí cloudu.

Technologie Active Directory byla navržena pro autentizaci a autorizaci v prostředí interní sítě. S nástupem moderních technologií v čele s cloudovými službami je stále častěji nutné řešit přesah autentizace i do tohoto prostoru.

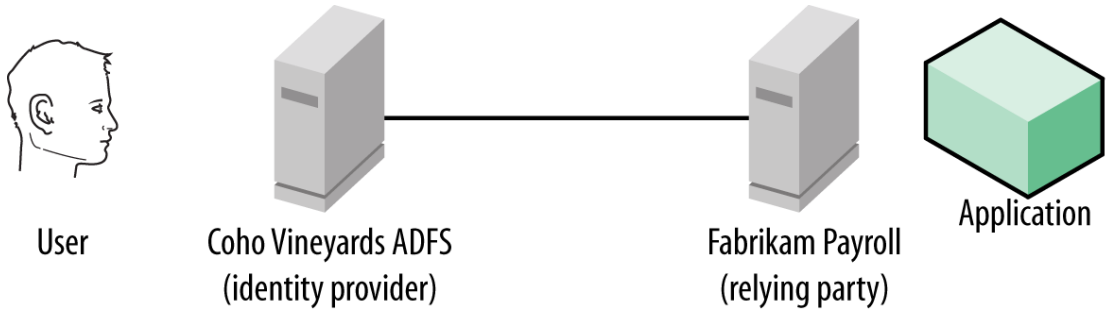
3.5 Active Directory Federation Services

ADFS je samostatná služba, která nese značku Active Directory, přirozeně se tak očekává, že správci Active Directory budou připraveni k nasazení a správě tohoto produktu. Ve skutečnosti je však ADFS vlastní produkt, který byl jen zařazen po bok Active Directory technologie.

3.5.1. Úvod do federace identit

Myšlenka federace identit je, že jedna strana (poskytovatel identity, identity provider, dále IdP) bude moci potvrdit identitu (autentizovat) uživatele druhé straně (Relying party – dále RP).

Mějme například následující situaci: organizace Coho Vineyards zadá zpracování mzdové agendy zaměstnanců jiné firmě – Fabrikam Payroll. Společnost Fabrikam Payroll provozuje webový portál pro zaměstnance. Aby bylo možné získat přístup k tomuto portálu, kde uživatelé najdou informace o jejich mzdách, daních atd., je potřeba najít způsob, jak se přihlásit do portálu Fabrikam Payroll, který je umístěn v datovém centru společnosti Fabrikam Payroll. Následující obrázek popisuje tento scénář. Uživatelé existují v AD prostředí společnosti CohoVineyard. CohoVineyard nasadila prostředí ADFS a je v tomto případě poskytovatelem identit – IdP. Coho Vineyard a Fabrikam Payroll mají mezi sebou vytvořen federační vztah důvěryhodnosti. V tomto případě je webová stránka Fabrikam Payroll relying party - RP.



Obrázek 14- Přehled Federace (2)

Princip fungování federace identit

Existuje několik protokolů, které se používají pro výměnu informací mezi partnery ve scénářích federace identit. Dva nejpoužívanější jsou:

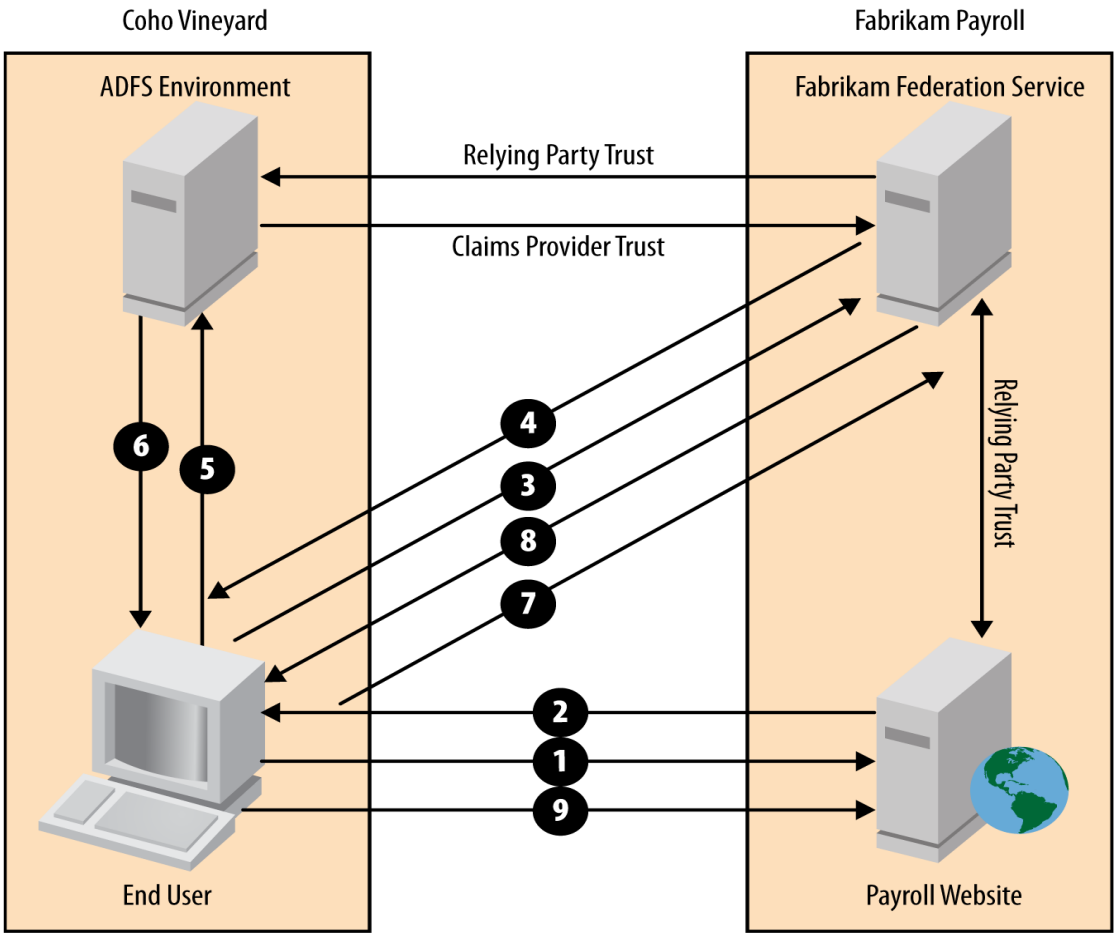
- Security Assertion Markup Language (SAML)

- WSFederation (WS-Fed)

SAML a WS-Fed z konceptuálního pohledu fungují obdobně, liší se formátování dat. V obou případech IdP generuje XML (Extensible Markup Language) fragment, který obsahuje řadu tvrzení (claim) o daném uživateli. Claimy jsou jednoduše atributy s hodnotou. Běžné příklady jsou uživatelské jméno, e-mailová adresa, číslo zaměstnance a tak dále. Tento soubor claimů rozšířený o další podpůrná data v XML formátu dává vzniknout tzv. uživatelskému tokenu pro přístup k RP. RP používá tvrzení v tokenu k autorizaci uživatele. (10)

Aby bylo možné zaručit, že token byl vydán IdP a že s ním nebylo manipulováno, IDP digitálně podepíše XML token pomocí jeho podpisového certifikátu. RP vlastní kopii veřejného klíče podpisového certifikátu IdP a tak může po tom, co obdrží token od IdP, použít veřejný klíč k potvrzení, že token je platný. Celý tento proces je založen na principech asynchroního šifrování, kdy k zašifrování obsahu je použit privátní klíč certifikátu, který má k dispozici pouze vlastník certifikátu – v tomto případě IdP. K rozšifrování je potom použit pouze veřejný klíč tohoto certifikátu, který naopak vlastní RP. Tímto způsobem lze ověřit, že token byl odeslán opravdu ze strany IdP a že s ním nebylo po cestě manipulováno – jinak by nemohl být zašifrován privátním klíčem certifikátu IdP.

Příklad, kdy chce uživatel přistupovat na webové stránky Fabrikam Payroll, je znázorněn na následujícím obrázku.



Obrázek 15- Tok zpráv v případě federace identit. (2)

Tento scénář obsahuje následující kroky, aby uživatel získal přístup k portálu Fabrikam

1. Uživatel přejde na webovou stránku Fabrikam Payroll pomocí webového prohlížeče. Na webových stránkách Fabrikam mezd se uživatel pokusí o přihlášení a aplikace zjistí, že uživatel musí být přihlášen přes federaci.
2. Na webových stránkách vydá přesměrování HTTP do uživatelova prohlížeče a nasměruje ho na stránku URL Federační služby společnosti Fabrikam
3. Uživatel pomocí webového prohlížeče přejde na federační službu společnosti Fabrikam.
4. Tato Federační služba společnosti Fabrikam vyhledá URL pro IdP společnosti Coho Vineyard a vydá přesměrování HTTP do uživatelova prohlížeče.
5. Uživatel pomocí webového prohlížeče přejde na federační službu společnosti Coho Vineyard.

6. Uživatel se autentizuje ADFS serveru a je mu vrácen token, který je podepsán pomocí token signing certifikátu a následně je uživatel přesměrován zpět na federační službu společnosti Fabrikam
7. Prohlížeč uživatele předloží token získaný v minulém kroku federační službě společnosti Fabrikam.
8. Tato federační služba společnosti Fabrikam tento token ověří a poté vydá uživateli nový token pro přístup na webové stránky Fabrikam Payroll, který je podepsán token signing certifikátem federační služby společnosti Fabrikam, a konečně federační služba společnosti Fabrikam přesměruje klienta na stránku Fabrikam Payroll
9. uživatel přistupuje na webové stránky Fabrikam Payroll a předkládá token vydaný federační službou společnosti Fabkrikam. Webová stránka ověří token, autorizuje uživatele a umožní mu přístup do aplikace.

Ačkoliv tento proces vypadá krkolomně a složitě, je ve skutečnosti velmi rychlý a efektivní. Některé kroky jsou dané podmínkami federační služby. Webová stránka, případně obecně jakákoliv aplikace, k níž klient přistupuje, může důvěřovat pouze jedné federační službě. Federační služba na druhé straně může ovšem důvěřovat libovolnému počtu poskytovatelů identit. Webový portál Fabrikam Payroll navštěvuje mnoho uživatelů z různých AD prostředí. Proto tato aplikace důvěřuje federační službě spol. Fabrikam a následně tato federační služba obsahuje další poskytovatele identit (Coho Vineyards a další zákazníky – každý další zákazník je vytvořen jako další poskytovatel identit)

V některých případech webové stránky nebo aplikace fungují také jako služba federace identit. V tomto případě je vztah důvěryhodnosti navázán přímo mezi ADFS serverem zákazníka a webovou stránkou. To odstraňuje několik skoků v procesu výše, ale funkčně je to totožné.(10)

V kroku 6 je uživateli prezentován token podepsaný ADFS serverem Coho Vineyards. Vzhledem k tomu, že vztah důvěry mezi Coho Vineyard a Fabrikam Payroll je mezi federačními službami, uživatel musí předložit podepsaný token zpět na federační službu spol. Fabrikam (krok 7). Federační služba spol. Fabrikam potom ověří token a pokud vše souhlasí, vydá nový token, který je podepsán certifikátem Fabrikam (krok 8). Vzhledem k tomu, že aplikace Fabrikam Payroll důvěřuje pouze federační službě ve spol. Fabrikam, webová stránka by nemohla ověřit token, kdyby byl podepsán pomocí ADFS serveru Coho VineYards.

Koncepty fungování nástrojů na federaci identit jsou podobné jako dříve popisovaný protokol Kerberos; identity provider je v tomto případě obdoba doménového řadiče, resource provider je v tomto případě obdoba aplikačního serveru (např. Souborového serveru). Při přístupu k aplikaci musí uživatel předložit federační tiket (obdoba servisního tiketu v protokolu Kerberos). Servisní tiket v protokolu Kerberos je šifrován pomocí hashe hesla servisního účtu služby a podobně je v systému federace identit šifrován federační token certifikátem federační služby.

SAML

Security Assertion Markup Language (SAML) 2.0 je jeden ze dvou primárních norem pro přenos federačních tokenů mezi prostředími. V USA převládá SAML v oblasti vzdělávání a vládních organizací a je také používán v mnoha aplikacích třetích stran a cloudových služeb. Pro externí cloudové služby je podpora SAML logickou volbou pro dosažení širokého spektra kompatibility se systémy potenciálních zákazníků. Specifikace pro SAML jsou k dispozici online. Dokumentace obsahuje ve velké míře termín „assertion“. V SAML je termín „assertion“ funkčně ekvivalentní výrazu "Token" používanému dříve v této kapitole.

WS-Federation

WS-Federation je protokol používaný společností Microsoft ve svých aplikacích a vývojových sadách softwaru (SDK). První verze ADFS podporovala dokonce pouze WS-Federation. To byl problém, který výrazně ovlivnil přijetí ADFS, jelikož pro velkou část trhu byly nepřístupné tím, že využívala SAML. .NET aplikace postavené pomocí Windows Identity Foundation (WIF) nebo .NET Framework 4.5 obecně používají WS-Fed ve svých interakcích s IdP.

3.5.2. ADFS komponenty a topologie nasazení

V této kapitole jsou popsány jednotlivé komponenty technologie ADFS a nastíněny jednotlivé topologie nasazení pro prostředí různých velikostí.

Konfigurační databáze

První rozhodnutí, které je nutné udělat před nasazením ADFS, je zvolení místa, kam se bude ukládat konfigurace ADFS. Existují dvě místa, kde ADFS může ukládat své konfigurační informace – do interní databáze systému Windows (WID) instance, která je replikována na každý federační server, nebo ve sdíleném prostředí na SQL Server. Obě možnosti mají výhody i nevýhody. Databáze WID je velmi jednoduché nasadit (WID je součástí systému Windows) a není potřeba žádné dodatečné licence. WID také odstraňuje jediný bod selhání v distribuovaném prostředí ADFS. Při použití WID každý federační server obsahuje kopii konfigurační databáze. Jeden z federačních serverů (Obvykle první Federační server, který byl nasazen) se označuje jako "primární" server. Všechny změny konfigurace se provádí na primárním serveru a tyto změny jsou potom replikovány na všechny ostatní federační servery každých pět minut.

Databáze WID má také několik omezení. Zaprvé, pokud jde o výkon a kapacitu v extrémně velkých prostředí ADFS, a dále ukládání konfigurace do WID odstraňuje podporu pro další funkce SAML, jako je rozlišení artefaktu a detekce token replay útoku.

SAML artefakty jsou funkce specifické pro SAML (oproti WS-Fed). SAML artefakty dovolují SAML tokenům (tvrzením, claimům) poskytovat ukazatel na kus dat, které lze nezávisle na sobě použít bez nutnosti jejich vložení do SAML tvrzení. Vzhledem k tomu, že žádost o načtení artefaktu přijde později a žádost by mohla dorazit do jiného federačního serveru, artefakty musí být uloženy v konfigurační databázi, aby byly k dispozici i ostatním serverům.

Detekce token replay útoků zajišťuje, že token, který je vydán ADFS, nelze znovu použít. ADFS ukládá informace o každém tokenu, který vydá, do konfigurační databáze, aby bylo zajištěno, že token není následně znovu použit. Tato funkce také vyžaduje, aby konfigurační databáze byla uložena ve sdíleném prostředí SQL Server oproti WID databázi.

A konečně, pomocí prostředí založeném na SQL Serveru, je možné využít funkcí vysoké dostupnosti SQL, jako je clustering a zrcadlení. Tyto funkce mohou být užitečné při tvorbě scénářů využívajících několik geografických lokalit pro zajištění redundance.

Federační servery

Federační server je srdcem a duší prostředí ADFS. Federační servery jsou schopné působit jako IdP i jako RP v závislosti na scénáři.

Správné zabezpečení (jak fyzické, tak logické) federačního serveru je velmi důležité. Federační servery jsou stejně jako řadiče domény důležité tím, že kontrolují přístup k aplikacím a službám. Každý, kdo má přístup k federačnímu serveru, by se mohl vydávat za kteréhokoliv uživatele v organizaci vytvořením falešného tokenu, který je podepsán podepisovacím certifikátem federačního serveru. Pro druhou stranu by tento token byl validní a autentický, protože by byl podepsán důvěryhodným certifikátem.

Proxy federačního serveru

Proxy federačního serveru je volitelná funkce, která se používá k vytvoření dodatečné vrstvy mezi federační servery a internet. Funkčně proxy neumí nic, co by nemohl dělat federační server. Existují ale některé situace, ve kterých je výhodné použít proxy federačního serveru.

Hlavní možnost, kterou proxy federačního serveru umožňuje, je mít různé autentizační mechanismy pro interní a externí uživatele. Když se uživatelé připojí vnitřně k federačnímu serveru v podnikové síti za účelem získání tokenu, je možné se spolehnout na integrované ověřování systému Windows (Kerberos a NTLM), které umožní projít přes ADFS bez jakýchkoliv dalších výzev. Nicméně externě mohou uživatelé například používat své domácí počítače, které nejsou pod kontrolou IT, u kterých tudíž není známo, v jakém jsou stavu; mohou být neaktualizované, zavirované a tak dále. Nebo například uživatel může být připojený v kavárně na špatně zabezpečenou wifi, kde dalších několik lidí může vidět síťový provoz odcházející z uživatelova zařízení. V tomto případě bude pravděpodobně lepší volbou použít HTML formulář pro autentizaci uživatele.

Proxy federačního servery také izolují externí klienty od poměrně citlivých dat na federačním serveru – privátních klíčů, které se používají k podpisu tokenů. To poskytuje další úroveň zabezpečení.

Některé organizace se rozhodnou použít reverzní proxy server jiný než proxy federačního serveru k publikaci svých ADFS serverů do internetu, jiní se rozhodnou zveřejňovat své federační servery přímo na internetu. Microsoft doporučuje používat proxy federačního serveru v jeho dokumentaci.

Topologie ADFS

Existuje několik topologií pro nasazení technologie ADFS od malých a jednoduchých až po velké, komplexní a vysoce redundantní.

Důležitými aspekty při volbě příslušné topologie nasazení technologie ADFS jsou požadavky na rozšiřitelnost a případně vysokou dostupnost této služby. Jakmile bude ADFS technologie začleněna do procesu ověřování uživatelů při přístupu ke službám, jakýkoliv výpadek této služby způsobí okamžitou nedostupnost dané služby, do níž se uživatel autentizuje pomocí ADFS, ačkoliv služba samotná bude fungovat bez problémů dále, při nedostupnosti ADFS serverů se nebude možné k této službě přihlásit.

Toto je běžný vývoj v mnoha organizacích, které se rozhodnou využívat cloudové služby z důvodů vysoké dostupnosti a také faktu, že se o tyto služby dále nemusí starat. Místo toho se ale starají, aby služba ADFS běžela neustále a bez výpadku.

Jeden federační server

Nejjednodušší topologie vhodná pro testování a vývoj zahrnuje nasazení pouze jednoho federačního serveru. V tomto případě se jen nainstaluje ADFS role na Windows Server a použije konfigurační průvodce k nasazení tohoto federačního serveru. Obvykle se pro tento scénář nepoužívá SQL server, ale místo toho se pro konfigurační databázi použije Windows Integrated Database. Mimo prostředí pro testování a vývoj je použití této topologie značně omezené.

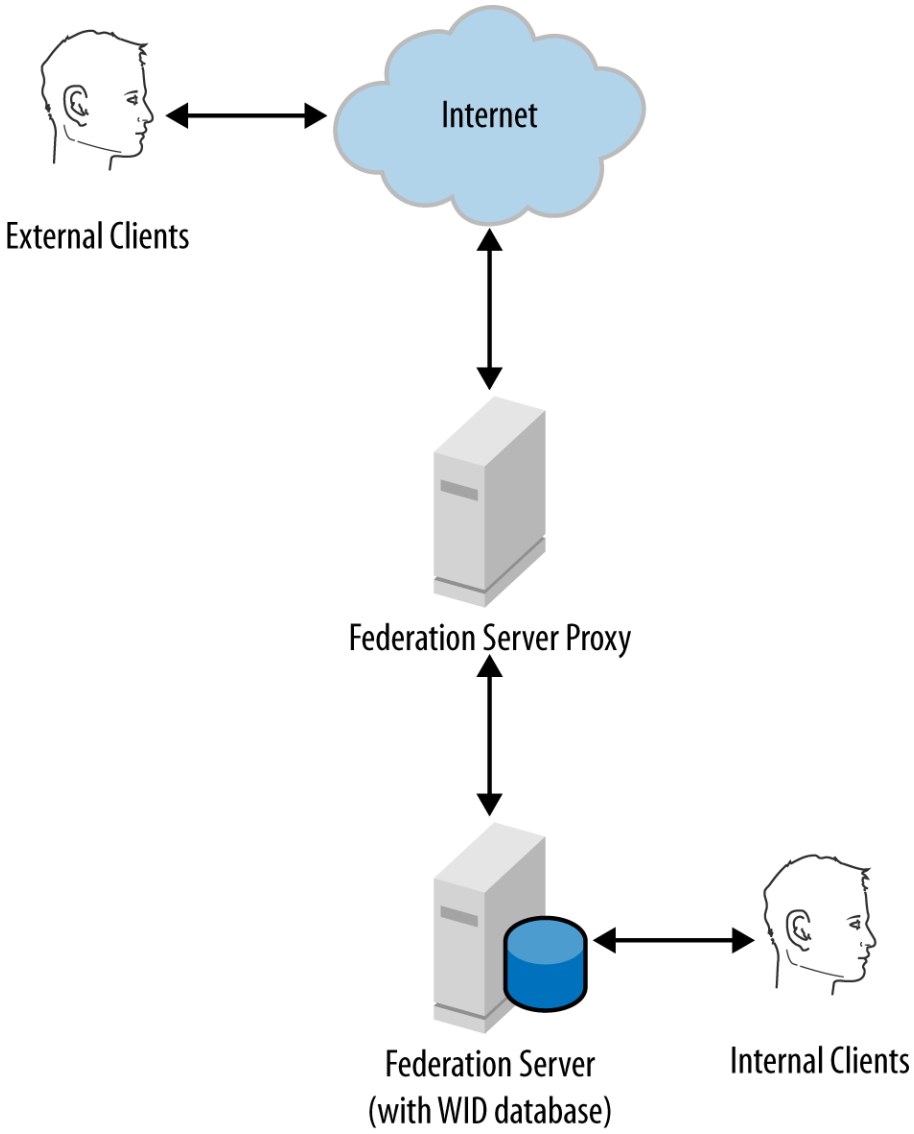
Jeden federační server ve spojení s federační proxy

V tomto případě jsou potřeba dva servery, jak ukazuje následující obrázek. Jeden server funguje jako federační server a hostuje konfigurační databázi a druhý server funguje jako federační proxy a publikuje služby ADFS do internetu.

Tato topologie je vhodná pro organizaci, která potřebuje federovat s jedním nebo více partnery, a zároveň aplikace, u níž se používá ADFS k ověřování, nevyžaduje vysokou dostupnost na úrovni serveru. Vysoká dostupnost může být řešena jiným způsobem, například geograficky, to ale záleží na konkrétním případě. Tato topologie umožňuje relativně snadnou rozšiřitelnost o další servery proxy, případně o další federační servery, pokud to bude v budoucnu potřeba. Databáze může být uložena i na SQL serveru, pokud je vyžadována podpora SAML artefaktů, případně detekce replay útoků.

ADFS servery s rozložením zátěže (load-balanced)

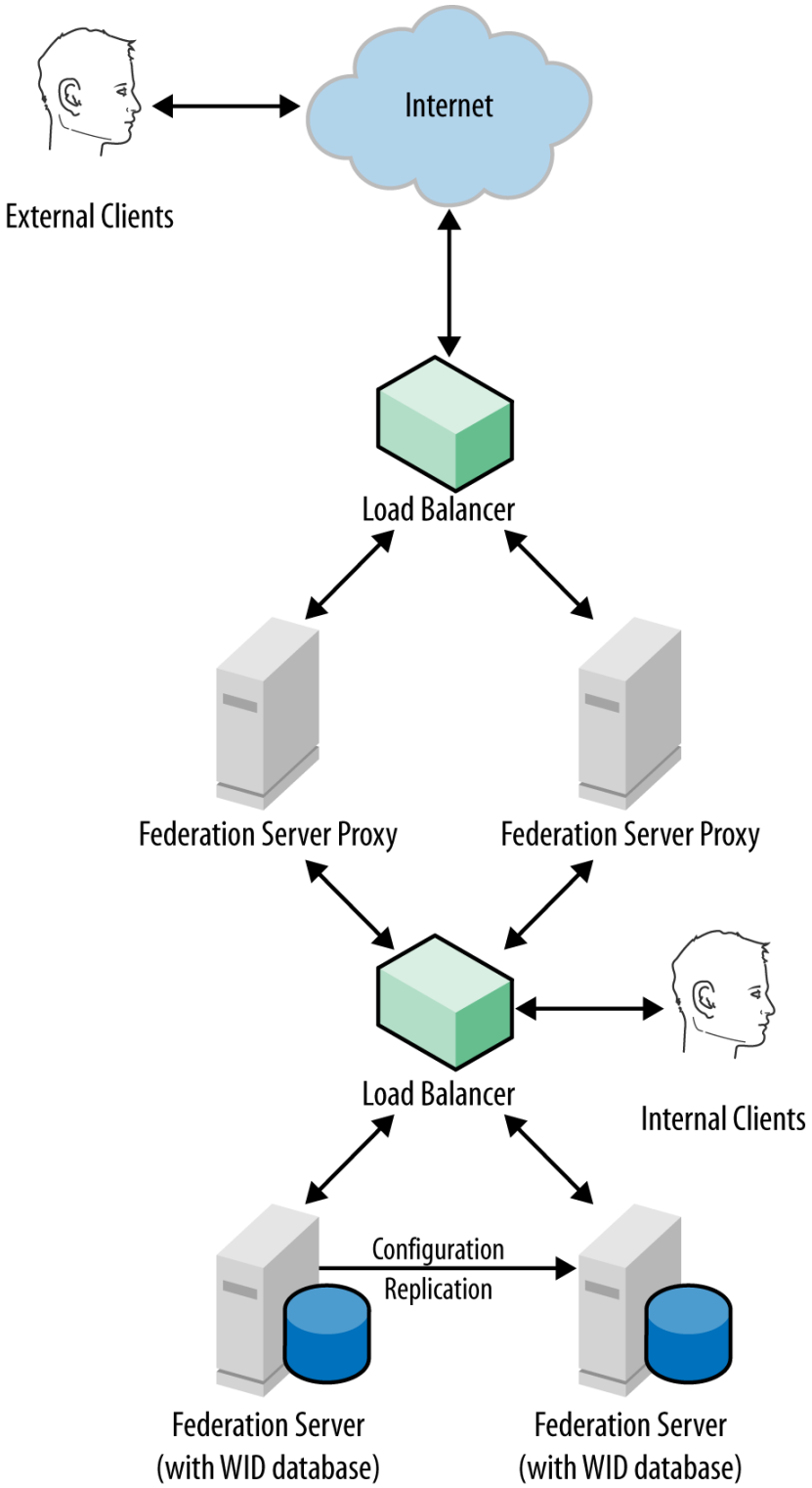
Pokud z nějakého důvodu existuje požadavek na redundanci komponent ADFS, je potřeba zahrnout do návrhu řešení také technologii load-balancing. Toto bude pravděpodobně vyžadovat kooperaci několika týmů zároveň, jelikož je nutná úprava konfigurace síťových zařízení. Ačkoliv samotná konfigurace load-balancingu není složitá, je nutné nastavit load-balancing na vrstvě 4 pro porty 80 a 443 na síťovém zařízení.



Obrázek 16- Scénář bez zvýšené dostupnosti (2)

I když je možné použít komponentu Windows Network Load Balancing, která je součástí windows, obecně se pro tyto účely doporučuje použít spíše některý z hardwarových load-balancerů. (6)

Následující obrázek zobrazuje standardní topologii s load-balancerem. V tomto případě jsou součástí topologie dva servery proxy, které využívají load-balancer, a dále další dva servery, které fungují jako federační servery taktéž využívající load balancer. V tomto případě je pro uložení konfigurační databáze použita Windows Internal Database, ale je samozřejmě možné použít SQL server z důvodů již zmíněných, případně z důvodu požadavku na vysokou dostupnost nebo výkon.



Obrázek 17- Topologie s load balancerem (2)

Ačkoliv diagram zobrazuje použití dvou separátních load balancerů, jinou variantou je také vytvoření dvou virtuálních IP na jednom load balanceru. Toto záleží na konkrétním prostředí

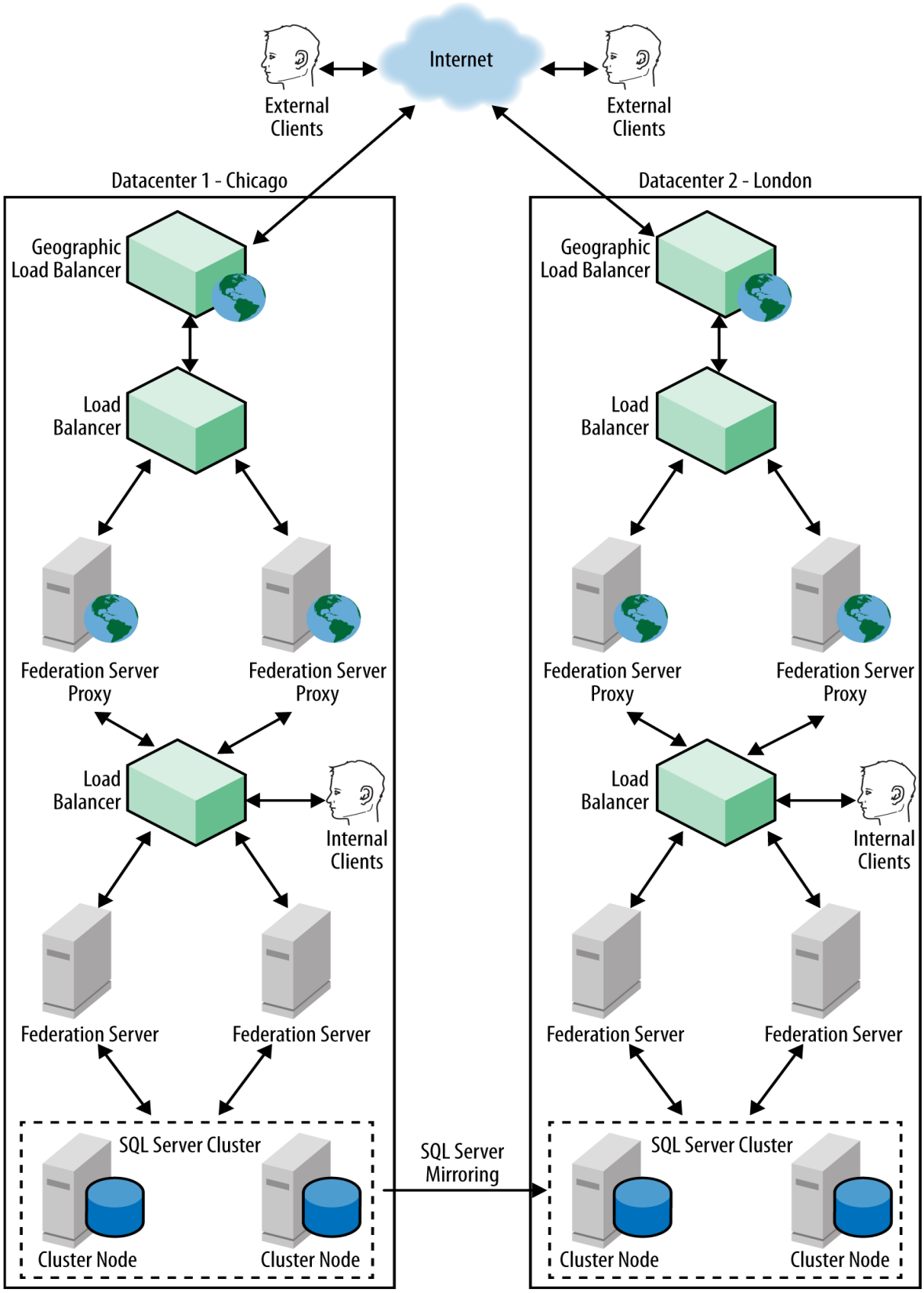
a je to jedno z témat, které by mělo být prodiskutováno se síťovým týmem před samotným nasazením služby.

Geograficky redundantní implementace ADFS

Poslední a nejkomplexnější topologie zahrnuje umístění ADFS serverů do několika geografických lokalit tak, aby byla zaručena nejvyšší úroveň dostupnosti. V tomto případě je nutné nasadit také technologii, která umožní, že DNS název ADFS služby bude přeložen na IP adresu, která je nejblíže danému klientovi.

Aby bylo možné dosáhnout geografické redundance služby, bude kromě load balancerů v lokálních datacentrech nutné použít i technologii pro load balancing na úrovni celých datacenter. Na trhu existuje několik služeb, které toto umožňují.

Krom samotného řešení load balancingu bude nutné také využít funkcionalit SQL serveru, a to konkrétně zrcadlení a replikaci konfigurační databáze do jednotlivých datacenter, která hostují dané ADFS prostředí. (6)



Obrázek 18- implementace geografickeho load balancingu s ADFS službou (1)

4. Vlastní práce

Vlastní práce je založena na implementaci dvou scénářů nasazení služby Active Directory v laboratorním prostředí a identifikaci vhodného řešení pro každou danou situaci.

Scénáře nasazení jsou založeny na prostředí fiktivní společnosti, jejíž parametry (velikost, technické vybavení, způsob používání IT prostředků, velikost rozpočtu pro IT) jsou zvoleny na základě osobních zkušeností autora tak, aby co nejlépe vystihovaly nejčastější typ společnosti řešící situaci popsanou daným scénářem nasazení. Parametry společnosti byly vybrány s ohledem na lokální trh České Republiky.

4.1 Charakteristika firmy

Společnost ABC použitá ve vlastní části působí jako výrobce bazénů a zastřešení se sídlem v České Republice. Společnost ABC působí jak na lokálním trhu, tak na trzích v okolních zemích, a to hlavně na Slovensku, v Rakousku a Německu. Společnost má sídlo v Praze, výrobní závod v Pardubicích a Liberci a několik desítek obchodních zastoupení napříč Českou Republikou. Společnost ABC ovládá většinu lokálního trhu s bazény v ČR. Na centrále v Praze pracuje přibližně sto stálých zaměstnanců. Výrobní závody a obchodní zastoupení zaměstnávají dohromady dalších sto zaměstnanců.

4.1.1. Informační Technologie

Společnost ABC využívá servery na platformě Windows a Linux. Adresářovou službu zajišťuje technologie Active Directory, která tvoří doménu abc.cz. Dále jsou využívány poštovní služby produktu Microsoft Exchange, souborové služby, webové služby na platformě IIS, databázový server s Microsoft SQL serverem a terminálový server s ERP a CRM aplikacemi.

Klientské počítače jsou zastoupeny jak stolními počítači, tak notebooky. Na stolních počítačích běží operační systém Microsoft Windows, přibližně na polovině ve verzi Windows 7 a na druhé polovině ve verzi Windows 10. Notebooky jsou zastoupeny jak počítači s Windows 10, tak počítači Apple MacBook.

V sídle společnosti v Praze je provozována serverovna, která obsahuje několik serverů dle následující tabulky:

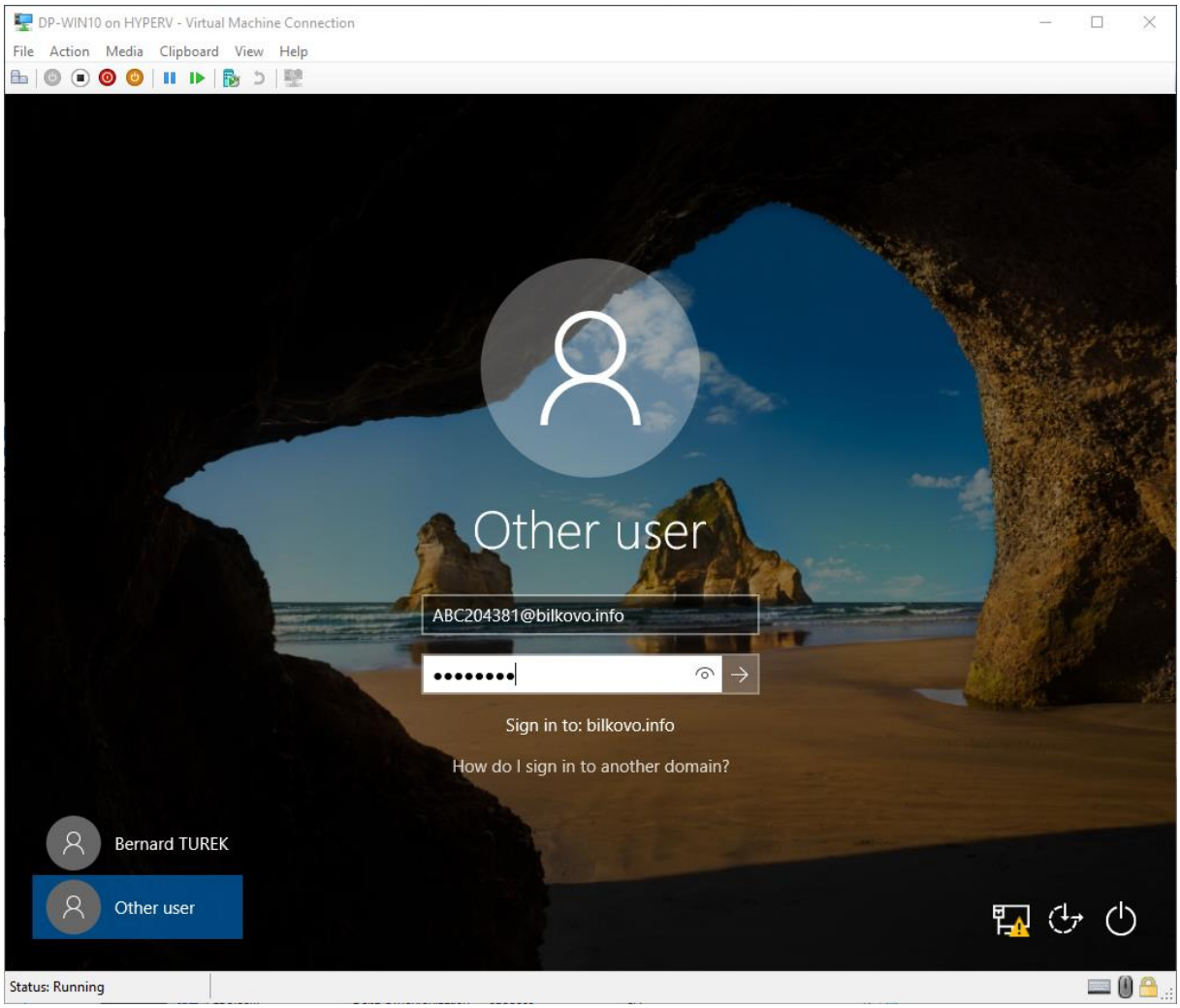
Název Serveru	Operační Systém	Role
AD1	Windows 2012R2	Řadič domény AD – fyzický
AD2	Windows 2012R2	Řadič domény AD – virtuální
SRV1	Windows 2012R2	Poštovní server Exchange
DHCP1	Windows 2012R2	DHCP server
SQL1	Windows 2012R2	SQL server
TS1	Windows 2012R2	Terminálový Server
IIS1	Windows 2012R2	Webový server
IIS2	Windows 2012R2	Webový server
APACHE1	Centos Linux	Webový server
FILE1	Windows 2012R2	Souborový server
HV1	Windows 2016	Hypervizor
HV2	Windows 2016	Hypervizor
HV3	Windows 2016	Hypervizor

Tabulka 7- Servery ve společnosti ABC

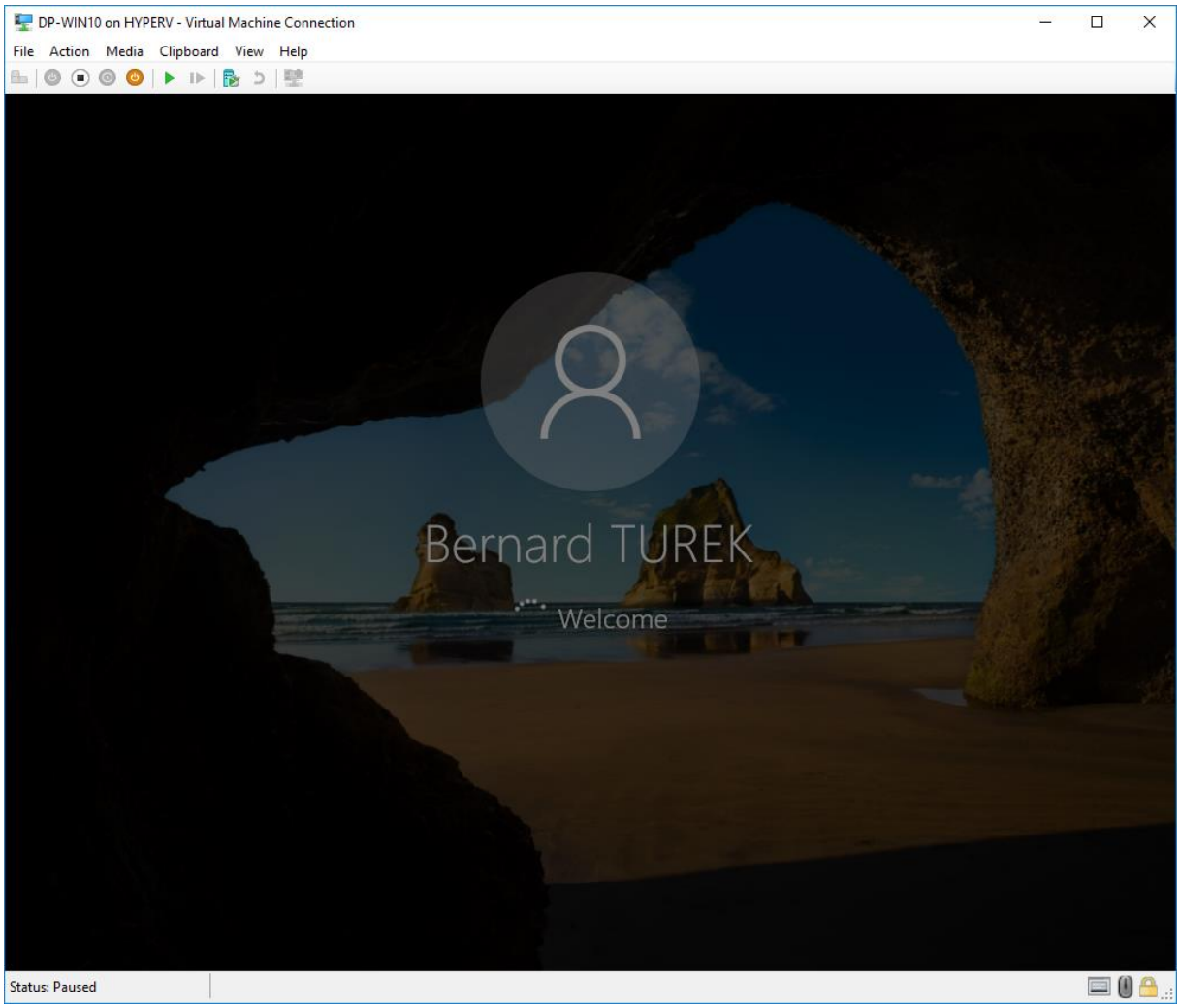
Jednotlivé pobočky obsahují vždy řadič domény Active Directory, a to v plné variantě v případě větších poboček, u kterých je zajištěna akceptovatelná úroveň fyzického zabezpečení serverů, případně ve verzi Read Only Domain Controller (RODC) u menších poboček s horšími možnostmi fyzického zabezpečení serverů. Dále pak souborový server.

Některé pobočky dále obsahují další obslužné servery – například pobočka v Liberci provozuje server pro obsluhu stroje pro lisování a docházkový server.

V současné době se uživatelé společnosti ABC přihlašují ke zdrojům v síti pomocí uživatelského jména a hesla v doméně Active Directory. Uživatelské jméno je tvořeno jedinečným identifikátorem (zaměstnaneckým číslem) a UPN příponou, kterou společnost ABC používá v prostředí internetu (bilkovo.info). Uživatelské jméno potom může vypadat například takto: ABC204381@bilkovo.info a toto jméno uživatelé používají pro přihlašování ke klientským stanicím, jak je znázorněno na následujících obrázcích.



Obrázek 19- Přihlášení pomocí alternativního UPN – přihlašovací dialog



Obrázek 20- Přihlášení pomocí alternativního UPN – přihlašování

Tento scénář byl zvolen proto, že velká část prostředí Active Directory byla vytvořena ještě před rozšířením internetových služeb a proto velmi často název domény Active Directory neodpovídá názvu, který společnost používá v prostředí internetu. V tomto případě doména abc.cz použitá pro interní Active Directory doménu neodpovídá doméně bilkovo.info, kterou firma používá pro prezenci na internetu.

4.2 Laboratorní prostředí

Laboratorní prostředí bylo z větší části virtualizované na platformě Microsoft Hyper-V nasazené na HW platformě Dell VRTX.

Laboratorní prostředí bylo vytvořeno s cílem co nejvěrněji napodobit prostředí společnosti ABC, zvláště potom konfiguraci a způsob používání autentizačních mechanismů technologie Active Directory.

V laboratorním prostředí byli vytvořeny servery potřebné pro nasazení technologie Active Directory.

Role Active Directory byla nakonfigurována s ohledem na charakteristiky společnosti. V Active Directory byly pomocí skriptovacího jazyka PowerShell vytvořeny fiktivní uživatelské objekty. Skript využívá externí databázi křestních jmen a příjmení zvlášť pro ženy a muže. Tato databáze byla naplněna údaji s nejčetnějšími jmény a příjmeními v České Republice dle údajů z Českého Statistického Úřadu. Dále skript používá externí databázi náhodných adres v České Republice a databázi telefonních předvoleb.

Cloudová část laboratorního prostředí je reprezentována službami Microsoft Azure, konkrétně službou Azure Active Directory. Technologie Azure Active Directory je používána pro ověřování uživatelů přistupujících ke cloudovým službám na platformě Azure a také ke službám Office 365.

4.3 Scénář 1 – Active Directory a služba v cloudu

Společnost ABC se rozhodla stávající řešení poštovních služeb se serverem Microsoft Exchange postupně nahradit cloudovými službami Office 365. Tomuto rozhodnutí předcházel projekt zhodnocení výhodnosti přechodu na Office 365.

Mezi důvody přechodu na Office 365 patří:

- Snížení zátěže na internetovou konektivitu Pražské centrály,
- Zjednodušení infrastruktury,
- Snížení zátěže IT pracovníků – nemusí se starat o infrastrukturu poštovních serverů,
- Lepší antispamová ochrana než při stávajícím řešení,
- Větší velikost poštovní schránky pro uživatele.

Zachování tohoto způsobu přihlašování je hlavním požadavkem pro nové řešení ověřování.

Tento požadavek může být splněn pomocí dvou odlišných technologií, na kterých jsou následně založeny implementované scénáře nasazení:

4.3.1. Synchronizace identit a hesel pomocí nástroje ADConnect

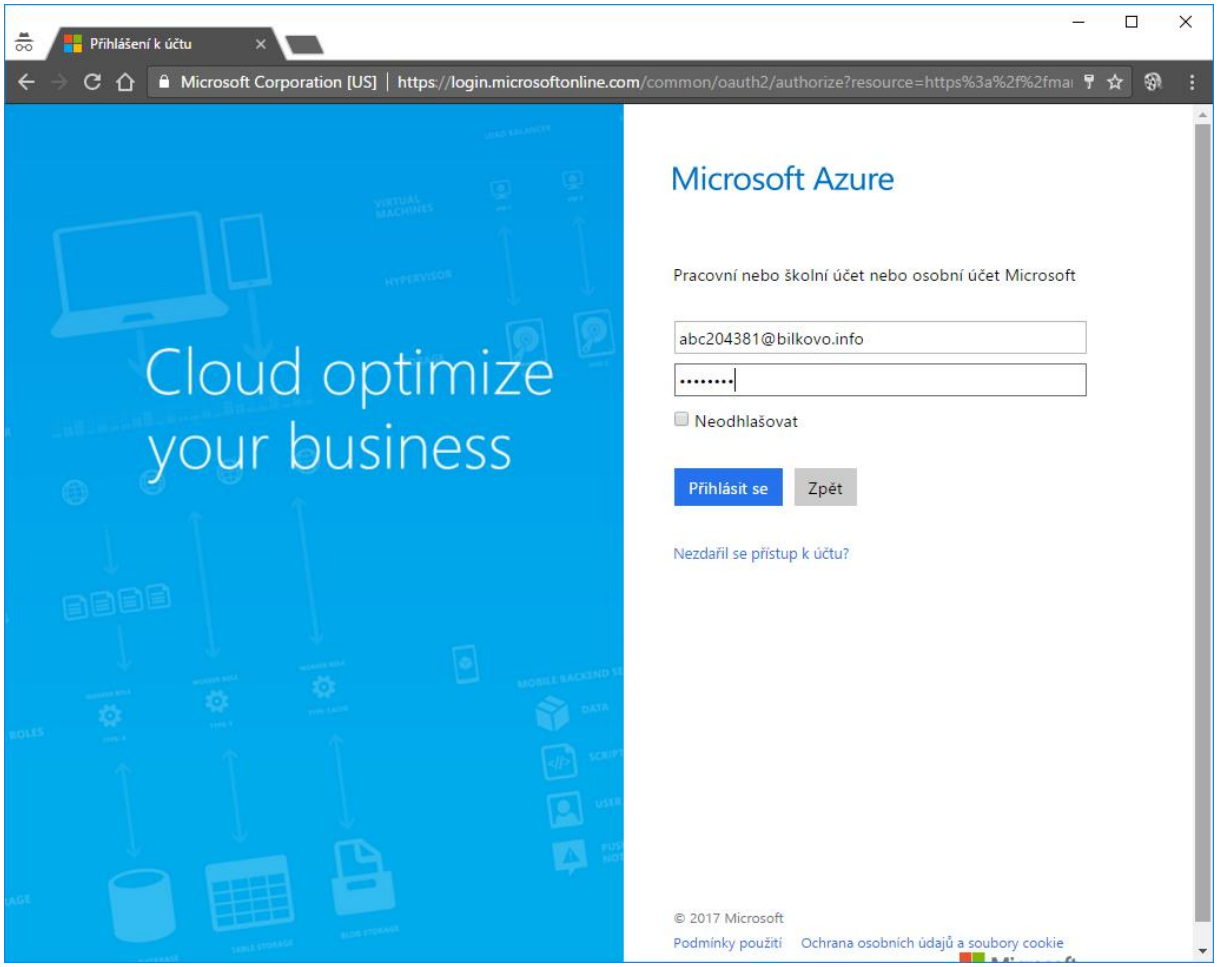
Nástroj ADConnect je volně stažitelná aplikace, umožňující sychronizaci identit mezi prostředím Active Directory a Azure Active Directory. Nástroj ADConnect navazuje na své předchůdce, nástroje AD Sync a DirSync. ADConnect je založen na jádře z vyspělejšího produktu Microsoft Identity Management, avšak neumožňuje pokročilejší nastavení.

4.3.1.1. Implementace ADConnect v prostředí ABC

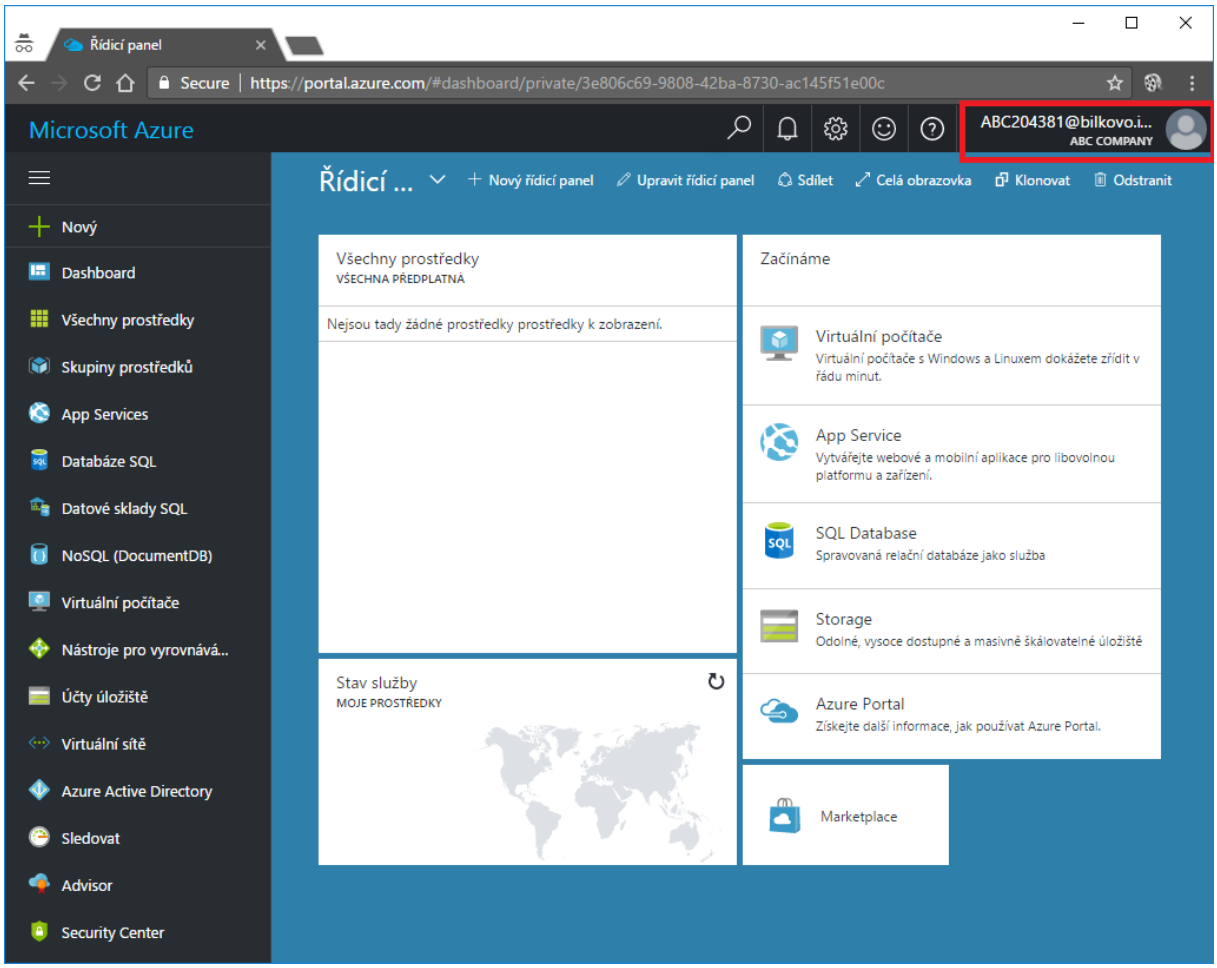
V prostředí společnosti ABC bylo nutné zřídit nový virtuální server pro provoz tohoto nástroje. Ačkoliv dle dokumentace, není instalace tohoto nástroje přímo na doménový řadič výslovně zakázána, nedoporučuje se z důvodu bezpečnosti. ADConnect vyžaduje přístup k internetu, který je pro doménové řadiče ve společnosti ABC zakázán. Z těchto důvodů bylo nutné vytvořit nový server pro účely nástroje ADConnect.

Instalace a konfigurace nástroje ADConnect zahrnuje vytvoření virtuálního stroje a instalaci operačního systému. Následně byl nainstalován nástroj ADConnect, s použitím doporučené konfigurace, která zahrnuje synchronizaci identit současného AD lesa ABC.COM včetně synchronizace všech dostupných atributů a také synchronizaci hesel z prostředí Active Directory do cloudové služby Azure Active Directory.

Po nasazení nástroje ADConnect a provedení úvodní synchronizace bylo možné provést přihlášení ke zdroji v cloudu pomocí uživatelského jména a hesla, které uživatel používá pro přihlášení ke svému klientskému počítači. Přihlášení je znázorněno následujícími obrázky.



Obrázek 21- Přihlášení do cloudové aplikace pomocí UPN – přihlašovací dialog



Obrázek 22- Přihlášení do cloudové aplikace pomocí UPN – úspěšné přihlášení

4.3.2. Využití Active Directory Federation Services

Druhou možností, jak vyřešit ověřování uživatelů je využití technologie Active Directory Federation Services (ADFS). V případě využití technologie Active Directory Federation Services je uživatel po zadání uživatelského jména ihned přesměrován na autentizační stránku společnosti ABC, na které zadá heslo. Uživatel, ačkoliv se přihlašuje ke cloudové službě, je ověřen serverem, který je pod kontrolou společnosti ABC.

Výhodou tohoto řešení je, že heslo samotné nikdy neopouští servery společnosti ABC, není nijak synchronizováno do jiné adresářové služby tak jako je tomu v případě použití nástroje ADConnect se synchronizací hesel. Další výhodou je fakt, že Active Directory Federation Services infrastruktura může být použita i pro další účely, nejen ověřování v cloudových službách, ale také například ve scénáři sdílení dat mezi společnostmi, jak popisuje scénář 2.

Nevýhodou je závislost autentizační platformy na funkčnosti Active Directory Federation Services infrastruktury. V případě nefunkčnosti některé z částí Active Directory Federation Services infrastruktury nebude fungovat přihlášení ke službám v cloudu. Toto se týká i samotného internetového připojení ADFS serverů. Pokud dojde k výpadku internetového připojení, nebude možné doručit autentizační požadavek z cloudové služby na službu Active Directory Federation Services a ověření selže. Z tohoto důvodu je nutné plánovat toto řešení s přihlédnutím k těmto vlastnostem a požadované dostupnosti řešení.

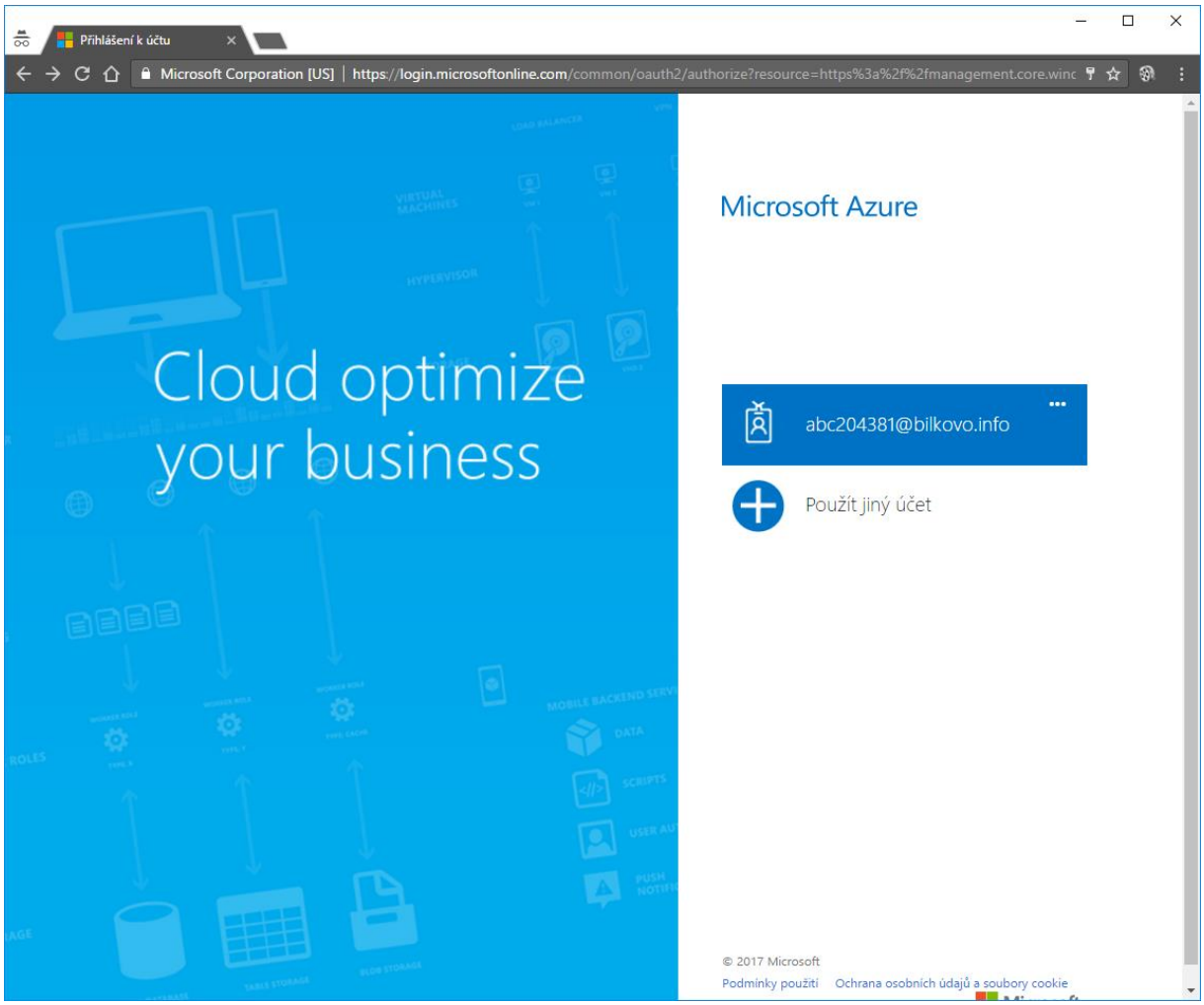
4.3.2.1. Implementace ADFS v prostředí ABC

Nasazení technologie ADFS je možné dvěma způsoby. První způsob, do nedávna jediný možný, spočívá v nainstalování role Active Directory Federation Services a následně její manuální konfigurace. Nástroj ADConnect však umožňuje automatizovanou instalaci a konfiguraci prostředí ADFS. Potřeba jsou 2 servery, jeden pro samotný ADFS server a druhý pro ADFS proxy.

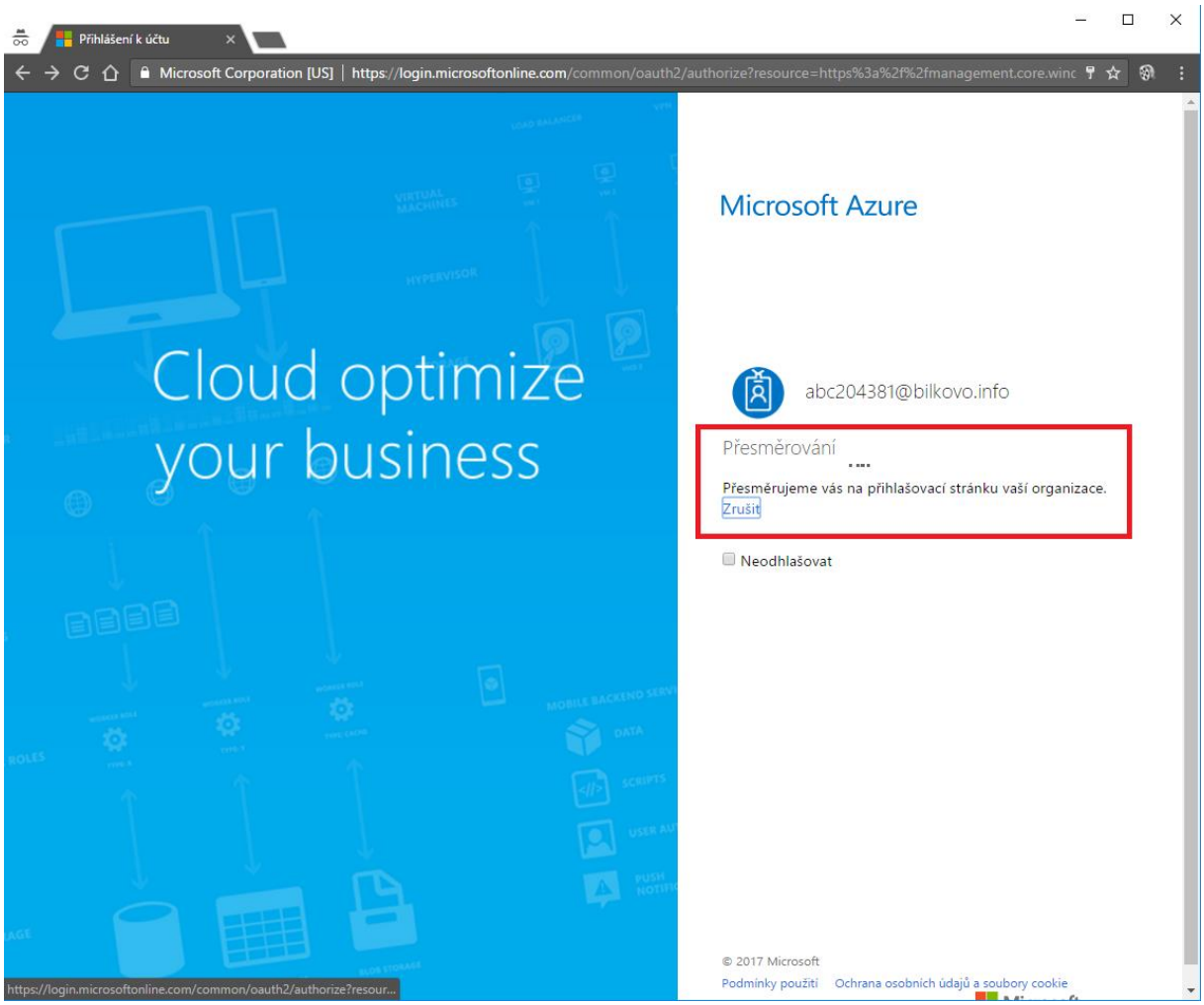
Součástí konfigurace ADFS infrastruktury je i pořízení důvěryhodného certifikátu pro ověřovací portál. Tento certifikát by měl být vydán důvěryhodnou certifikační autoritou. Při konfiguraci pomocí nástroje ADConnect je třeba poskytnout tento certifikát ve formátu *.pfx. Včetně privátního klíče. Certifikát musí být vystaven s jménem, pod kterým bude ADFS služba dostupná z internetu – v tomto případě sts.bilkovo.info.

Konfigurace sítě zahrnuje vytvoření záznamu v externím DNS pro záznam sts.bilkovo.info a jeho nasměrování na veřejnou IP adresu routeru společnosti ABC. Následně je nutné přesměrovat port 443 na lokální adresu ADFS Proxy serveru, tak aby byl ADFS proxy server dostupný pod internetovou adresou sts.bilkovo.info.

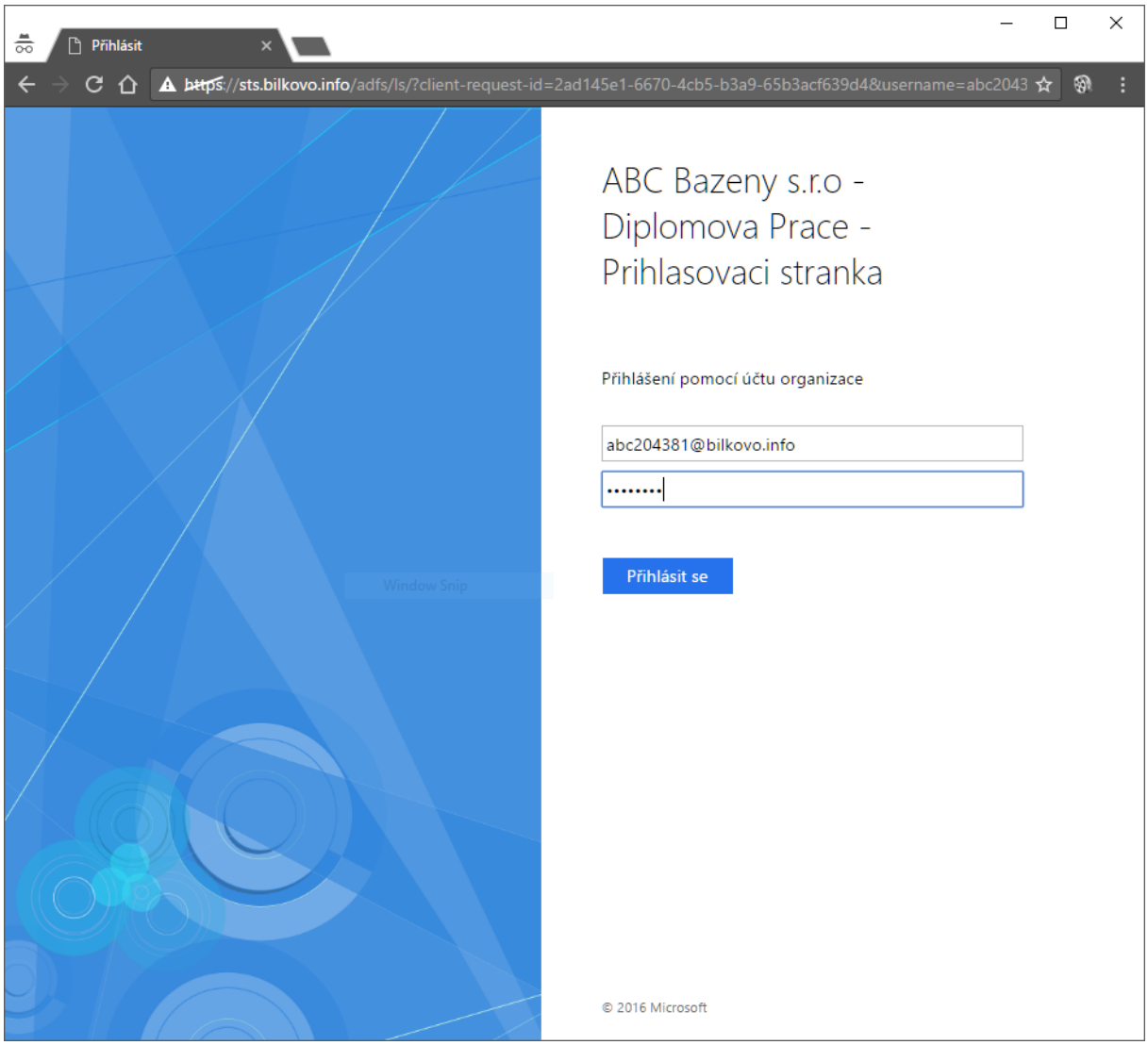
Po konfiguraci ADFS infrastruktury se změní chování přihlašovacího dialogu do cloudové služby. Po zadání uživatelského jména (v tomto případě abc204381@bilkovo.info – obrázek 23) dojde k přesměrování na přihlašovací stránku organizace – tato přihlašovací stránka již běží na ADFS Infrastruktuře společnosti ABC(obrázek 24).



Obrázek 23- Přihlašovací dialog



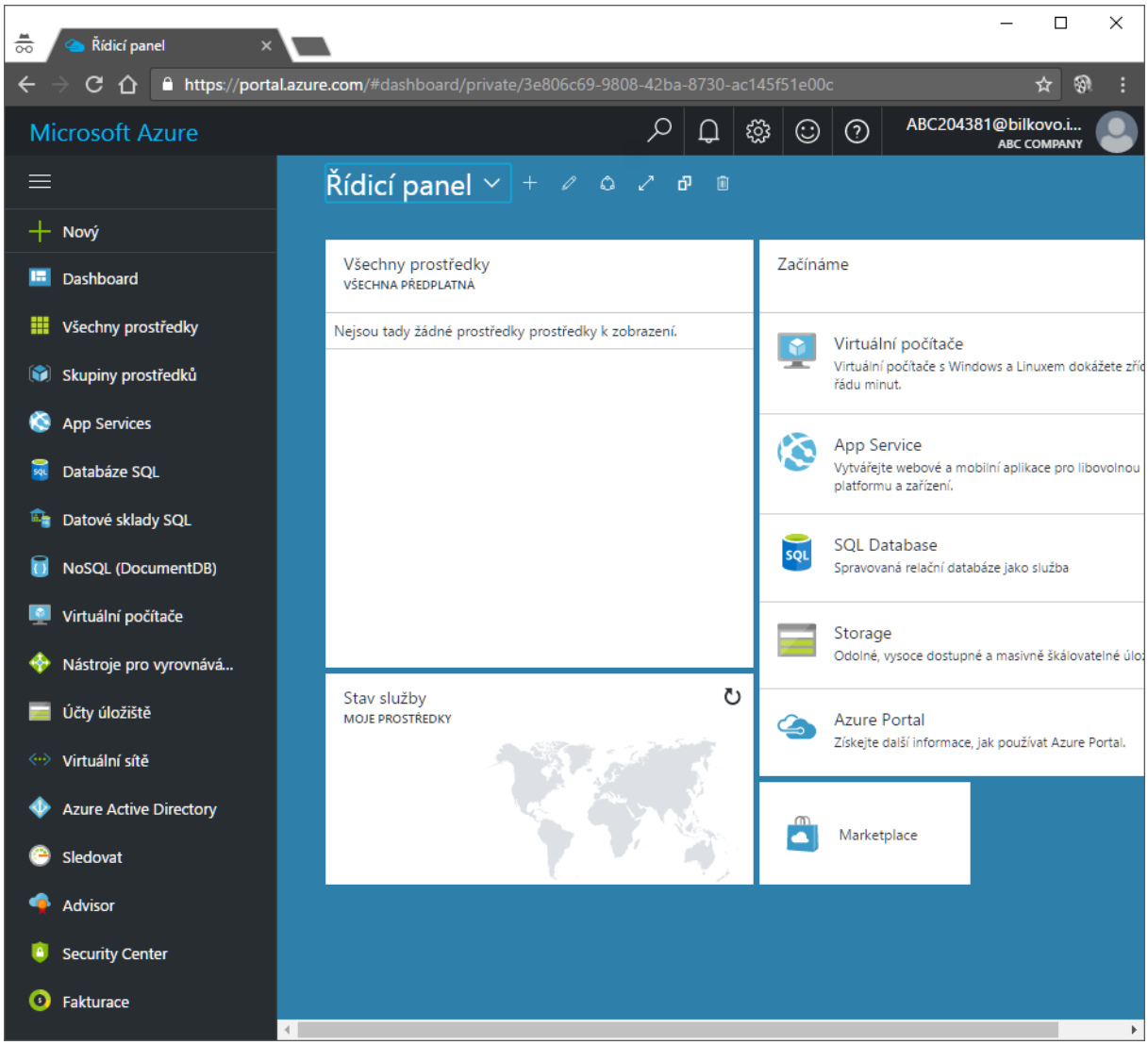
Obrázek 24- Přesměrování na přihlašovací stránku organizace



Obrázek 25- přihlášení na přihlašovací stránce organizace

Přihlašovací stránku je možné přizpůsobit. Změna názvu společnosti byla provedena pomocí následujícího PowerShell příkazu (8):

```
Set-AdfsGlobalWebContent -CompanyName "ABC Bazeny s.r.o - Diplomova Prace - Prihlasovaci stranka"
```



Obrázek 26- úspěšné přihlášení

4.4 Scénář 2 – Sdílení přístupu k datům

V tomto scénáři došlo ke spojení společnosti ABC se společností BCD. Společnost ABC chce jako součást spojení firem umožnit společnosti BCD přístup do interní aplikace skladového hospodářství.

Požadavkem je zachování funkcionality Single Sign On tak, aby uživatelé ze společnosti BCD mohli používat vlastní přihlašovací údaje k systému ve společnosti ABC.

Tento požadavek může být naplněn dvěma technologiemi, na kterých jsou následně založeny implementované scénáře nasazení:

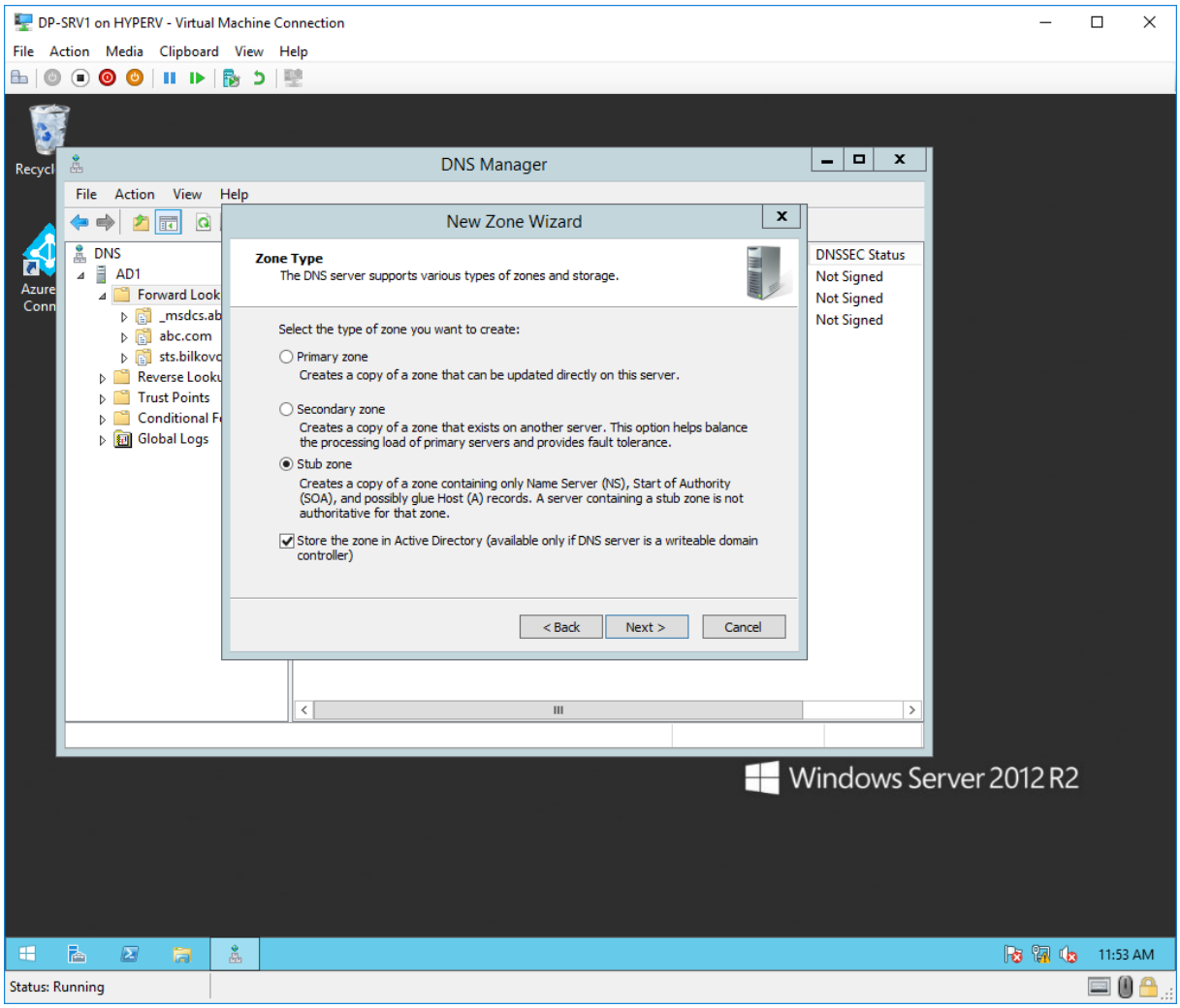
4.4.1. Varianta 1 - Active Directory trust mezi dvěma společnostmi

Active Directory trust, neboli vztah důvěryhodnosti mezi doménami, je původní technologie navržená pro sdílení identit mezi dvěma Active Directory prostředími. Vytvoření Active Directory trustu umožní uživateli z jednoho Active Directory prostředí přistupovat ke zdroji v jiném Active Directory prostředí. Ověřování tohoto uživatele probíhá na domovském doménovém řadiči a nedochází k žádné synchronizaci hesel.

Požadavkem na funkčnost Active Directory trustu je přímá konektivita mezi prostředími a také funkční překlad DNS jmen. Je nutné aby klienti z prostředí domény BCD dokázali správně přeložit jména z domény ABC.

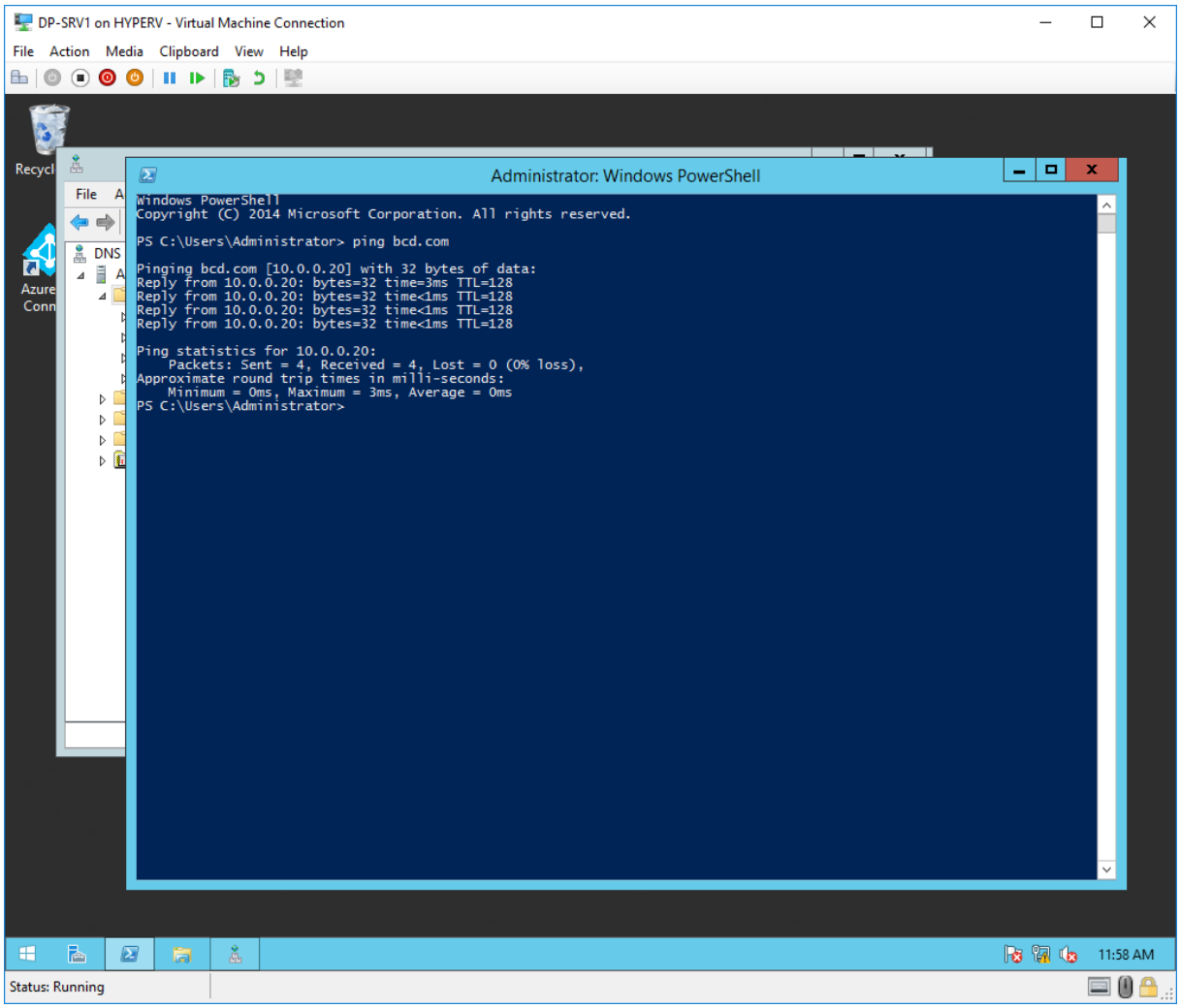
4.4.1.1. Implementace AD trust v prostředí společnosti ABC

Vytvoření Active Directory trustu v prostředí ABC zahrnovalo zajištění síťové konektivity mezi společnostmi ABC a BCD a to pomocí dedikované linky mezi oběma společnostmi. Dále implementace zahrnovala konfiguraci DNS záznamů na DNS serverech společnosti ABC, tak aby bylo možné zajistit spolehlivý překlad DNS adres z partnerské domény BCD. Tohoto cíle bylo dosaženo použitím stub zóny na DNS serverech v doméně ABC.COM.



Obrázek 27- vytvoření stub zóny v prostředí ABC

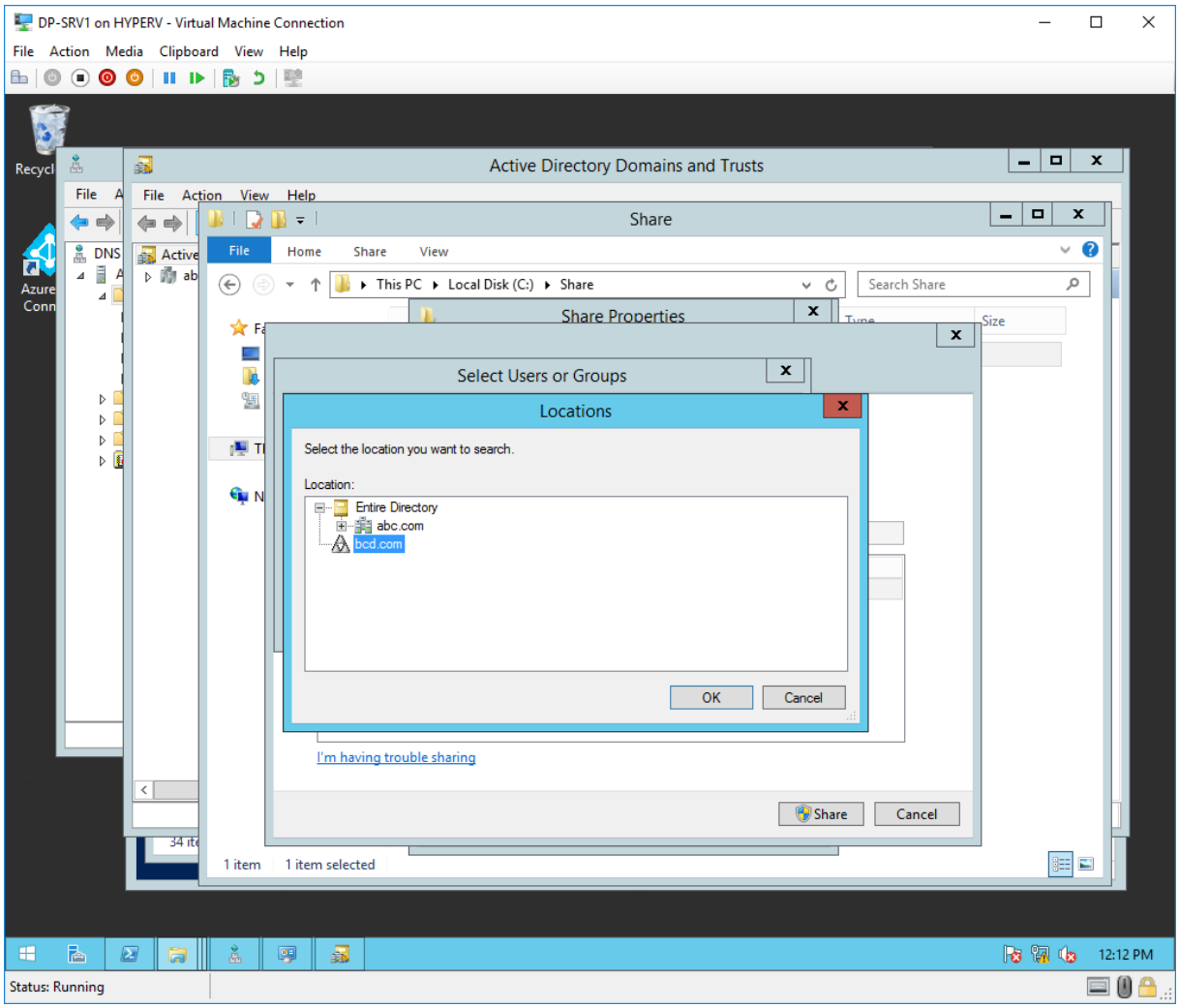
Po vytvoření stub zóny bylo možné překládat DNS záznamy domény BCD na strojích domény ABC.



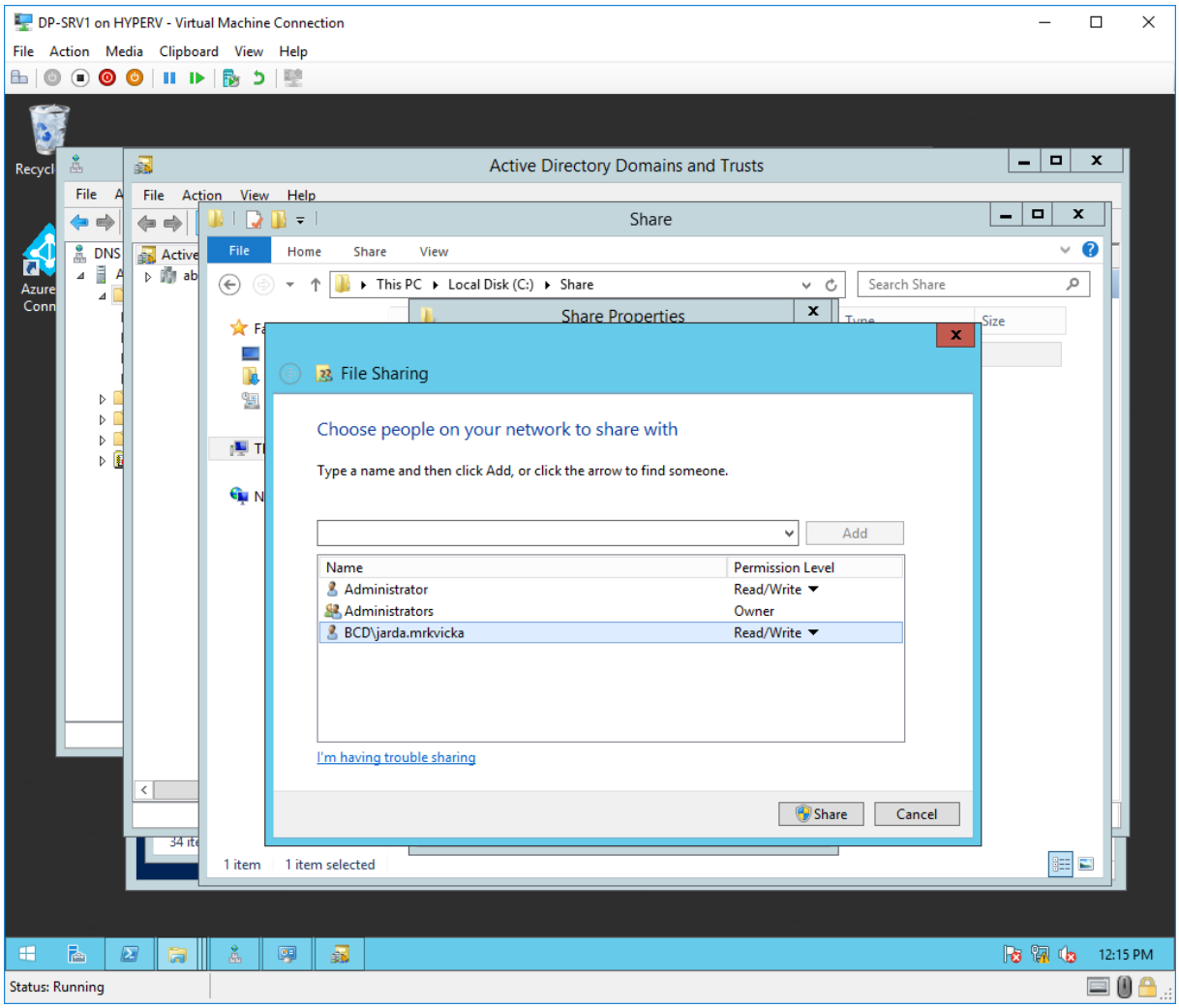
Obrázek 28- funční překlad DNS

Stejně tak na straně společnosti BCD bylo nutné provést kroky vedoucí k zajištění spolehlivého překladu DNS adres do domény ABC. Dále bylo nutné provést konfiguraci AD trustu na straně společnosti BCD.

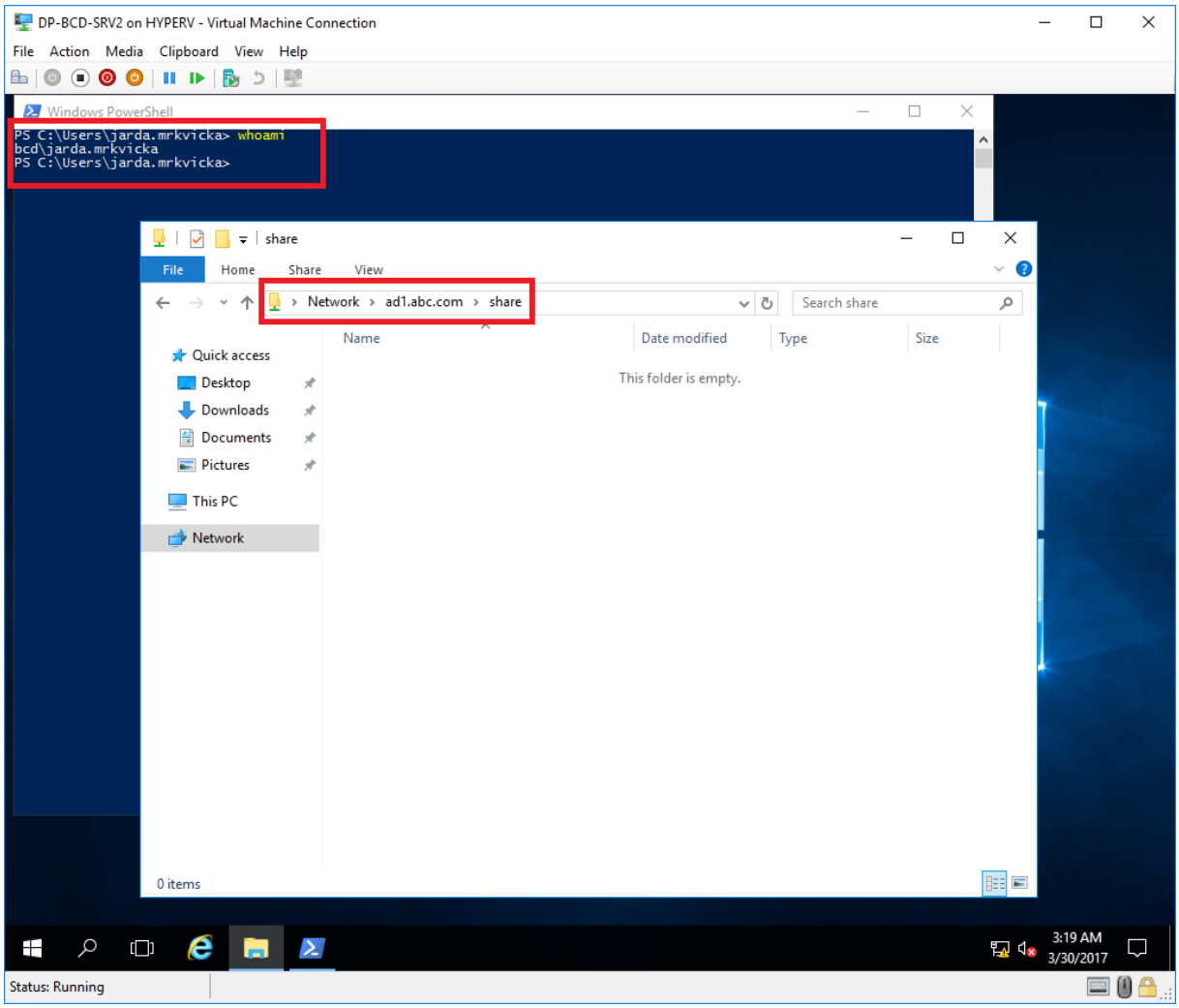
Po validaci trustu bylo možné přidat oprávnění na zdroj umístěný v doméně ABC i uživateli z domény BCD tak jak ukazují následující obrázky.



Obrázek 29- přidání oprávnění - doména BCD



Obrázek 30- Přiřazen přístup uživateli z domény BCD



Obrázek 31- funkční přístup k datům v doméně ABC uživatelem z domény BCD

Nasazení tohoto způsobu ověřování nevyžadovalo vytvoření žádného nového serveru. Jediná investice v tomto případě byla do dedikované síťové linky mezi oběma společnostmi. Vzhledem k fyzické blízkosti obou společností to byla preferovaná varianta. Další variantou je možnost vytvoření VPN propoje s využitím sítě internet, zde je však nutné investice do zařízení umožňující vytvoření šifrovaného VPN tunelu.

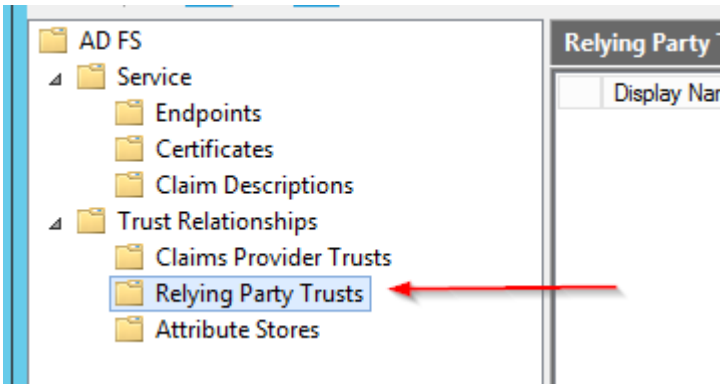
4.4.2. Varianta 2 - Využití Active Directory Federation Services

Stejně jako umožňují Active Directory Federation Services zprostředkovat autentizaci při přístupu ke zdrojům v cloudu jak bylo demonstrováno v druhé části prvního scénáře praktické části, je možné tuto technologii využít i pro ověřování mezi dvěma společnostmi. Výhodou oproti předchozí variantě je, že není potřebná přímá konektivita. Veškeré ověřování probíhá přes internet, podobně jako v druhé části prvního scénáře. Nevýhodou tohoto řešení je, že je nutná podpora ze strany aplikace. Aplikace musí podporovat tzv. Claim-aware autentizaci.

4.4.2.1. Implementace ADFS v prostředí společnosti ABC

V prostředí ABC bylo nutné nasadit dva servery. Jeden pro roli Active Directory Federation Services serveru a druhý jako Active Directory Federation Services Proxy. Podobně jako v případě implementace ADFS pro účely autentizace s cloudovou službou. Stejná infrastruktura je potřebná i na straně společnosti BCD.

Následně byl přidán na každé sraně tzv. „Relying Party Trust“, který definuje vztah důvěryhodnosti mezi jednotlivými stranami – v tomto případě společnost ABC a BCD. Ve společnosti ABC byl přidán trust se společností BCD. Tak aby se mohli uživatelé z domény BCD ověřovat na zdroji v doméně ABC.



Obrázek 32- Nastavení Relying Party Trustu

Ověřování následně probíhá obdobně jako v druhé části prvního scénáře.

5. Výsledky a diskuse

5.1 Scénář 1 – Active Directory a služba v cloudu

5.1.1. Varianta 1 - Synchronizace identit a hesel pomocí nástroje ADConnect

Synchronizace identit a hesel pomocí nástroje ADConnect nabízí jednoduchý způsob jakým umožnit uživatelům autentizaci v cloudových službách pomocí stejné sady přihlašovacích údajů, kterou používají v lokální síti. Řešení založené na nástroji ADConnect zároveň nabízí odolnost proti výpadku internetové konektivity – v případě výpadku internetové konektivity nebude možné synchronizovat změny, ale jelikož jsou identity a hesla plně synchronizována do cloudu stále bude možné se přihlásit ke zdroji v cloudu. Toto je vlastnost, kterou ostatní porovnávaná řešení nenabízí. Princip synchronizace identit má ale i své nevýhody, předně je to samotný fakt, že hesla opouští prostředí kontrolované společností. Tento fakt je nutné zohlednit při posuzování vhodnosti variant a ujistit se, že tím nedojde k porušení bezpečnostních politik organizace. K nevýhodám dále patří prodleva, která je daná synchronizačním cyklem. Pokud například dojde k zablokování uživatelského účtu z důvodu okamžité výpovědi zaměstnance, tato změna se v krajním případě může projevit až za nastavenou dobu synchronizačního cyklu (ve výchozím nastavení 30 minut). Uživatel s výpovědí tedy v krajním případě může ještě dalších 30 minut přistupovat k datům nebo službám v cloudu, ačkoliv jeho účet je v prostředí společnosti již zablokován.

Nasazení nástroje ADConnect je poměrně jednoduché, implementace tohoto řešení v laboratorním prostředí zabrala autorovi přibližně 12 hodin času. S připočtením rezervy a času potřebného k psaní dokumentace vstupuje do kalkulace 24 hodin času IT pracovníka. Kalkulace počítá s cenou 2500Kč za jednu hodinu práce IT pracovníka.

Výhody	Nevýhody
Jednoduchá konfigurace a nasazení	Hesla jsou synchronizována mimo prostředí společnosti
Odolnost prorti výpadkům internetového připojení	Prodleva při změně hesla
	Prodleva při změně oprávnění

Tabulka 8 - Scénář 1, Varianta 1 – Výhody a nevýhody

Náklady na infrastrukturu	
Nový server 1x	60000 Kč bez DPH (6)
Licence Windows Server	22193 Kč bez DPH (8)
Celková cena za infrastrukturu	82193 Kč bez DPH

Tabulka 9 - Scénář 1, Varianta 1 - Náklady na infrastrukturu

Náklady na práci	
Čas potřebný k nasazení	24 hodin
Hodinová sazba IT pracovníka	2500 Kč bez DPH
Celková cena za práci	**60000 Kč bez DPH**

Tabulka 10 - Scénář 1, Varianta 1 - Náklady na práci

Celkové náklady na nasazení řešení	
Náklady na infrastrukturu	82193 Kč bez DPH
Náklady na práci	60000 Kč bez DPH
Celková cena za nasazení řešení	**142193 Kč bez DPH**

Tabulka 11 - Scénář 1, Varianta 1 - Celkové náklady na nassazení řešení

5.1.1.1. Doporučení

V reálném prostředí mohou nastat problémy při synchronizaci objektů, které nemají unikátní některé atributy potřebné pro synchronizaci. Odstranění tohoto problému přináší další výdaje a proto autor doporučuje investovat do kontroly těchto atributů před nasazením tohoto nástroje.

5.1.2. Varianta 2 - Využití Active Directory Federation Services

Technologie Active Directory Federation Services odstraňuje nevýhody řešení založeného na nástroji ADConnect. Ověřování uživatele neprobíhá v cloudu, ale na serverech spravovaných společností ABC. Z tohoto důvodu nedochází k synchronizaci hesel a tím pádem hesla neopouští infrastrukturu ABC. Zároveň se tím eliminuje i prodleva popisovaná v předchozím scénáři nasazení. Změny jsou prováděny přímo na serverech, které provádějí samotnou autentizaci, proto jsou veškeré změny okamžité. Nevýhodou je, že pro samotnou autentizaci musí být ADFS služba dostupná klientovi. Což s sebou přináší jak závislost na připojení k internetu, tak závislost na funkčnosti služby a infrastruktury, na které běží, jako takové. Při navrhování ADFS infrastruktury je třeba zvážit požadavky na dostupnost této služby a případně zvážit některou z vysoce dostupných variant implentace služby ADFS, popisovaných v teoretické části práce. ADFS je obecně komplikovanější technologií než řešení na bázi nástroje ADConnect a synchronizaci hesel. Ačkoliv je nasazení této technologie díky automatizaci jednoduché, stále je pro účely řešení případných problémů nutné znát koncepty, na kterých ADFS funguje. To s sebou přináší další náklady na proškolení IT personálu, které v případě předchozí varianty zabere přibližně 1 hodinu, v tomto případě je pro pochopení ADFS nutné školení o délce minimálně 3 dny.

Nasazení technologie Active Directory Federation Services je díky modernizovanému nástroji ADConnect, který umožňuje provést automatizovanou instalaci Active Directory Federation Services poměrně jednoduché. Nástroj provede instalaci rolí na 2 servery, na Active Directory Federation Services server a Active Directory Federation Services Proxy. Při instalaci je potřeba doplnit certifikát včetně veřejného klíče, kterým se bude služba prezentovat. Implementace tohoto řešení v laboratorním prostředí zabrala autorovi přibližně 24 hodin. To zahrnuje přípravu dvou virtuálních serverů nad rámec standardního laboratorního prostředí, následně tvorbu certifikátu pro potřeby Active Directory Federation Services Proxy, následně nastavení externího DNS serveru a konfigurace interního síťového prvku. S připočtením rezervy a času potřebného k psaní dokumentace vstupuje do kalkulace 36 hodin času IT pracovníka. Kalkulace počítá s cenou 2500Kč bez DPH za jednu hodinu práce IT pracovníka. Následně je v kalkulaci počítáno i s absolvováním školení pro jednoho IT pracovníka o délce 3 dny s cenou 30000Kč bez DPH.

Výhody	Nevýhody
Hesla nejsou synchronizována mimo prostředí společnosti	Při výpadku služby ADFS nefunkční ověřování.
Žádné prodlevy při změnách	Obecně komplikovanější řešení
Možnost využít ADFS infrastrukturu i pro ověřování uživatelů dalších stran.	Nutné proškolení IT personálu

Tabulka 12 - Scénář 1, Varianta 2 - Výhody a nevýhody

Náklady na infrastrukturu	
Nový server 2x	120000 Kč bez DPH (6)
Licence Windows Server 2x	44386 Kč bez DPH (8)
Celková cena za infrastrukturu	164386 Kč bez DPH

Tabulka 13 - Scénář 1, Varianta 2 - Náklady na infrastrukturu

Náklady na práci	
Čas potřebný k nasazení	36 hodin práce
Hodinová sazba IT pracovníka	2500 Kč bez DPH
Celková cena za práci	**90000 Kč bez DPH**

Tabulka 14 - Scénář 1, Varianta 2 - Náklady na práci

Celkové náklady na nasazení řešení	
Náklady na infrastrukturu	164386 Kč bez DPH
Náklady na práci	90000 Kč
Náklady na proškolení správce IT	30000 Kč
Celková cena za nasazení řešení	**284386 Kč**

Tabulka 15 - Scénář 1, Varianta 2 - Celkové náklady na nasazení řešení

5.2 Scénář 2 – Sdílení přístupu k datům

5.2.1. Varianta 1 - Active Directory trust mezi dvěma společnostmi

Požadavkem na funkčnost Active Directory trustu je přímá konektivita mezi prostředími a také funkční překlad DNS jmen. Je nutné aby klienti z prostředí domény BCD dokázali správně přeložit jména z domény ABC. Což se ukázalo jako největší komplikace při nasazení této technologie. Pro zajištění spolehlivého překladu DNS jmen byla nutná konfigurace DNS infrastruktury, která přináší další náklady. Výhodou této varianty je určitá jednoduchost spočívající v absenci dedikovaných serverů pro tento účel, autentizace probíhá na stávajících řadičích domény Active Directory. Mezi výhody patří také širší podpora z pohledu aplikací, jelikož tento způsob autentizace využívá standardní protokoly NTLM a Kerberos. Síťová konektivita mezi prostředím firmy ABC a prostředím firmy BCD byla snadno nakonfigurována v laboratorním prostředí, nicméně v reálném světě může být zajištění konektivity velmi komplikované a může se stát rozhodujícím faktorem pro výběr technologie, do výpočtu byla zahrnuta cena 100 000kč bez DPH za vytvoření dedikované linky mezi oběma prostředími, a následně pravidelné platby za její správu ve výši 5000kč bez DPH měsíčně. Nasazení této varianty v laboratorním prostředí zabralo 10hodin, s přihlédnutím k nutné rezervě pro psaní dokumentace je v kalkulaci zahrnuto 24hodin práce IT pracovníka pro implementaci této varianty.

Výhody	Nevýhody
Není nutné pořizovat nové servery	Nutná přímá síťová konektivita mezi jednotlivými prostředími.
Žádné prodlevy při změnách	Nutná konfigurace DNS infrastruktury
Žádné speciální požadavky na podporu aplikací	

Tabulka 16 - Scénář 2, Varianta 1 - Výhody a nevýhody

Náklady na infrastrukturu	
Zřízení dedikované síťové linky	100000 Kč bez DPH a dále 5000kč bez DPH měsíčně za správu
Celková cena za infrastrukturu	100000 Kč bez DPH a dále 5000kč bez DPH měsíčně za správu

Tabulka 17- Scénář 2, Varianta 1 - Náklady na infrastrukturu

Náklady na práci	
Čas potřebný k nasazení	24 hodin práce IT pracovníka
Hodinová sazba IT pracovníka	2500 Kč
Celková cena za práci	**60000 Kč bez DPH**

Tabulka 18 - Scénář 2, Varianta 1 - Náklady na práci

Celkové náklady na nasazení řešení	
Náklady na infrastrukturu	100000 Kč bez DPH
Náklady na práci	60000 Kč bez DPH
Náklady na proškolení správce IT	160000 Kč bez DPH
Celková cena za nasazení řešení	**160000 Kč bez DPH**

Tabulka 19 - Scénář 2, Varianta 1 - Celkové náklady na nasazení řešení

5.2.2. Varianta 2 - Využití Active Directory Federation Services

V případě implementace technologie ADFS nebylo nutné vytvářet přímou konektivitu mezi jednotlivými prostředími. Technologie ADFS komunikuje prostřednictvím internetu. Absence dedikované linky může být považována za výhodu, ale zároveň tím nabývá na důležitosti kvalita připojení k internetu. Při výpadku připojení k internetu nebude možné provést autentizaci, protože ADFS služba přestane být dostupná z internetu. Vzhledem k charakteru služeb využívajících autentizaci přes ADFS je možné toto riziko zanedbat.

Implementace tohoto řešení zahrnovala instalaci dvou serverů pro každé prostředí. Pro každé prostředí byl nainstalován jeden ADFS server ve stejné síti s řadiči domény Active Directory, a také server Web Application Proxy nainstalovaný v síti DMZ a obsluhující požadavky z internetu, tak aby se zabránilo přístupu z internetu přímo na server ADFS.

Infrastrukturní nároky tedy zahrnují celkem 4 servery a jejich konfiguraci. Při instalaci je potřeba doplnit certifikát včetně veřejného klíče, kterým se bude služba prezentovat a to pro obě strany. Konfigurace ADFS infrastruktury v tomto případě zahrnuje konfiguraci na obou stranách, jak na straně společnosti ABC tak na straně společnosti BCD.

Implementace tohoto řešení v laboratorním prostředí zabrala autorovi přibližně 36 hodin. To zahrnuje přípravu čtyř virtuálních serverů nad rámec standardního laboratorního prostředí, následně tvorbu certifikátu pro potřeby Active Directory Federation Services Proxy, následně nastavení DNS infrastruktury a konfigurace interního síťového prvku. S připočtením rezervy a času potřebného k psaní dokumentace vstupuje do kalkulace 60 hodin času IT pracovníka. Kalkulace počítá s cenou 2500Kč bez DPH za jednu hodinu práce IT pracovníka. Následně je v kalkulaci počítáno i s absolvováním školení pro jednoho IT pracovníka o délce 3 dny s cenou 30000Kč bez DPH.

Ačkoliv je tato varianta výrazně dražší než varianta 1, jedná se o bezpečnější řešení, zejména díky absenci přímé konektivity mezi doménovými řadiči jednotlivých společností.

Výhody	Nevýhody
Není nutná přímá síťová konektivita mezi jednotlivými prostředími.	Při výpadku služby ADFS nefunkční ověřování.
Žádné prodlevy při změnách	Obecně komplikovanější řešení.
Možnost využít stejnou ADFS infrastrukturu i pro ověřování k prostředkům v cloudu.	Nutné proškolení IT personálu

Tabulka 20 - Scénář 2, Varianta 2 - Výhody a nevýhody

Náklady na infrastrukturu	
Nový server 4x	240000 Kč bez DPH (6)
Licence Windows Server 4x	88772 Kč bez DPH (8)
Celková cena za infrastrukturu	328772 Kč bez DPH

Tabulka 21 - Scénář 2, Varianta 2 - Náklady na infrastrukturu

Náklady na práci	
Čas potřebný k nasazení	60 hodin práce IT pracovníka
Hodinová sazba IT pracovníka	2500 Kč bez DPH
Celková cena za práci	**150000 Kč bez DPH**

Tabulka 22 - Scénář 2, Varianta 2 - Náklady na práci

Celkové náklady na nasazení řešení	
Náklady na infrastrukturu	328772 Kč bez DPH
Náklady na práci	150000 Kč bez DPH
Náklady na proškolení správce IT	30000 Kč bez DPH
Celková cena za nasazení řešení	**508772 Kč bez DPH**

Tabulka 23 - Scénář 2, Varianta 2 - Celkové náklady na nasazení řešení

6. Závěr

V práci byla formou literární rešerše uvedena historie technologie Active Directory, její začátek v dobách uzavřených počítačových sítí a její přerod v technologii fungující v prostředí cloudu a moderního IT.

Praktická část ukázala, že nasazení modernějšího způsobu autentizace uživatelů je v obou zamýšlených případech náročnější, jak na infrastrukturu, jelikož je třeba větší počet serverů, tak z pohledu pracnosti, kdy je třeba provést další konfigurační kroky.

Při hodnocení výsledků jen z pohledu nákladů vychází technologie ADFS v obou případech jako dražší. Při rozhodování je ale nutné zvážit další faktory, jako například bezpečnost. V obou případech je cenově výhodnější varianta zároveň také variantou méně bezpečnou, ať už v prvním scénáři, kdy je nutné sychronizovat hesla uživatelů do cloudové služby, tak i v případě druhého scénáře, kdy je zase nutné zajistit přímou konektivitu mezi řadiči domény Active Directory, což nemusí být vždy žádoucí.

Téma bezpečnosti může při volbě řešení zodpovědného za ověřování jmen a hesel a řízení přístupu k informacím hrát větší roli než možná finanční úspora.

Výpočet také ovlivňuje řada faktorů, jako například cena serverů a cena dedikované síťové linky pro propojení společností v případě druhého scénáře. V případě vysoce virtualizovaného prostředí, a přeneseně tedy s nižšími náklady na vytvoření nového serveru se situace může změnit ve prospěch modernější varianty autentizace.

7. Seznam použitých zdrojů

1. **Stanek, William.** *Active Directory: kapesní rádcea dministrátora.* místo neznámé : Computer Press, 2009.
2. **Desmond, Brian, Richards, Joe a Allen, Robbie.** *Designing, Depoloying, and Running Active Directory.* 2013.
3. **Allen, Robbie a Lowe-Norris, Alistair.** *Active Directory: implementace a správa Microsoft Active Directory.1.vyd.* 2005.
4. **Stanek, William.** *Mistrovství v Microsoft Windows Server 2008.* místo neznámé : Computer Press, 2009.
5. **Charlie, Russel.** *Deploying and Managing Active Directory with Windows PowerShell.* místo neznámé : Microsoft Press, 2015.
6. **Nickel, Jochen.** *Mastering Identity and Access Management with Microsoft Azure.* místo neznámé : Packt Publishing Limited, 2017.
7. **Hunter, Beau.** *Active Directory Field Guide.* místo neznámé : Springer, 2005.
8. **Yellapragada, Uma.** *Active Directory with PowerShell.* místo neznámé : Packt Publishing Limited, 2015.
9. **windows server pricing. [Online] Microsoft. [Citace: 15. 2 2017.] https://www.microsoft.com/cs-cz/cloud-platform/windows-server-pricing.**
10. Dell PowerEdge Configurator - Alza.cz. [Online] [Citace: 17. 2 2017.] https://www.alza.cz/dell-poweredge-r730-konfigurator-d3866664.htm.

8. Seznam obrázků

9. Seznam tabulek