Implementace zásad skupin pro doménu Microsoft Server ve společnosti Kovárna VIVA a.s.

Pavel Máčala

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel MÁČALA**
Osobní číslo:	**A10676**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Implementace zásad skupin pro doménu Microsoft Server ve společnosti Kovárna VIVA a.s.**

Zásady pro vypracování:

1. **Zpracujte literární rešerši k problematice Active Directory a zásad skupin v doméně Microsoft Server.**
2. **Analyzujte stávající stav.**
3. **Proveďte návrh využití a nastavení Active Directory.**
4. **Navrhněte využití a nastavení zásad skupin.**
5. **Zhodnoťte přínosy a náklady navržených řešení.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MOSKOWITZ, Jeremy. Group policy: fundamentals, security, and the managed desktop. Indianapolis, Ind.: Wiley, c2010. ISBN 04-705-8185-9.**
2. **STANEK, William R. Group Policy: zásady skupiny ve Windows : kapesní rádce administrátora. Vyd. 1. Brno: Computer Press, 2010, 351 s. ISBN 978-80-251-2920-3.**
3. **MALINA, Patrik. Jak vyzrát na Windows PowerShell 2.0: zásady skupiny ve Windows : kapesní rádce administrátora. Vyd. 1. Brno: Computer Press, 2010, 464 s. ISBN 978-80-251-2732-2.**
4. **STANEK, William R. Active Directory: kapesní rádce administrátora. Vyd. 1. Brno: Computer Press, 2009, 695 s. Kapesní rádce administrátora (Computer Press). ISBN 978-80-251-2555-7.**
5. **TULLOCH, By Mitch. Introducing windows server 2012 r2 rtm edition for it professionals. S.l.: Microsoft Press,U S, 2013. ISBN 978-073-5682-788.**

Vedoucí bakalářské práce:	**Ing. Petr Šilhavý, Ph.D.** Ústav počítačových a komunikačních systémů
Datum zadání bakalářské práce:	**28. února 2014**
Termín odevzdání bakalářské práce:	**13. června 2014**

Ve Zlíně dne 28. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

prof. Ing. Vladimír Vašek, CSc.
Za ředitel ústavu

ABSTRAKT

Tato bakalářská práce pojednává o návrhu a využití nastavení služby Active Directory a nastavení Group Policy v Microsoft Doméně. Cílem práce je co nevíce efektivně využít těchto nastavení v Kovárně VIVA a.s.

Klíčová slova:

Adresářová služba, Zásady skupiny, Windows server, Doména, Group Policy.

ABSTRACT

This bachelor thesis discusses the design and the usage of Active Directory settings and Group Policy settings in Microsoft Domain. The aim of the work is to use these settings most effectively in Kovárna VIVA Inc.

Keywords:

Active Directory, Group Policy, Windows server, Domain, Group Policy.

Poděkoval bych rád vedoucímu mé bakalářské práce panu Ing. Petru Šilhavému, Ph.D. za jeho rady a pomoc při jejím zpracování a Ing. Martinu Struhařovi za poskytnutí Workstation stanice, na které jsem testoval některá nastavení. Dále bych nechtěl opomenout poděkovat svému zaměstnavateli, firmě Kovárna VIVA a.s., která mi vycházela vstříc, pokud se jednalo o možnost úpravy pracovní doby v době zkoušek a přednášek na FAI UTB.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….……

podpis diplomanta

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 MICROSOFT WINDOWS SERVER 2012 ..... **11**
1.1 CO JE NOVÉHO VE WINDOWS SERVER 2012 R2 11
2 ACTIVE DIRECTORY **16**
2.1 SLUŽBA ACTIVE DIRECTORY 16
2.2 DOMÉNOVÉ SLUŽBY ACTIVE DIRECTORY 16
2.2.1 Rozhraní služby Active Directory 16
3 CO JE GROUP POLICY – SKUPINY ZÁSAD VE WINDOWS **22**
3.1 PRO CO SE GROUP POLICY POUŽÍVÁ 22
3.2 GROUP POLICY OBJECT "GPO" 22
3.3 DĚLENÍ POLICY "POLITIKY "' 22
3.3.1 Lokální politiky (Local Group Policy LGPO) 23
3.3.2 Doménové Politiky 24
3.4 HLAVNÍ VYUŽITÍ OBJEKTU DEFAULT DOMAIN POLICY 25
3.5 OVLIVNĚNÍ APLIKOVÁNÍ GPO POLITIK 25
3.6 DĚDIČNOST ZÁSAD SKUPIN 26
3.6.1 Změna pořadí propojení a priorita 27
3.7 GLOBÁLNÍ POLITIKY A ROZDĚLENÍ GPO 27
3.8 ZPŮSOB APLIKOVÁNÍ GPC (GROUP POLICY CLIENT) 28
3.8.1 Jak se GPO zpracovává při spuštění počítače a přihlášení uživatele 28
3.8.2 Výjimky při aplikování politik GPO 29
3.9 ŠABLONY A ADM A ADMX SOUBORY 30
3.9.1 Vyhledávání a filtrování v Administrative Templates 33
II PRAKTICKÁ ČÁST **34**
4 ORGANIZAČNÍ STRUKTURA SPOLEČNOSTI V NÁVAZNOSTI NA ACTIVE DIRECTORY **35**
4.1 PŘEDSTAVENÍ VNITŘNÍ SÍTĚ KOVÁRNY VIVA A.S. 36
4.2 VIRTUALIZAČNÍ SERVER FUJITSU RX300 S6 36
4.3 VIRTUALIZAČNÍ SERVER DELL POWEREDGE510 37
4.4 SOUHRN FYZICKÝCH A VIRTUÁLNÍCH SERVERŮ 38
5 ANALÝZA ACTIVE DIRECTORY - STÁVAJÍCÍ STAV **39**
5.1 NÁSTROJE PRO SPRÁVU SLUŽBY ACTIVE DIRECTORY 39
6 ANALÝZA ZÁSAD SKUPIN GPO (GROUP POLICY OBJECT) VE WINDOWS **42**
6.1 FILTRY ROZHRANÍ WMI(WINDOWS MANAGEMENT INSTRUMENTATION) 43
6.2 NÁVRH NA LEPŠÍ VYUŽITÍ A NASTAVENÍ ACTIVE DIRECTORY 43
7 NÁVRH, VYUŽITÍ A NASTAVENÍ ZÁSAD SKUPIN GPO **45**
7.1 TESTOVANÉ NASTAVENÍ ZÁSAD SKUPIN GPO 45
7.1.1 Čekání na síť pro Microsoft Windows XP 45

7.1.2 Windows Server Update Service (WSUS) 46
7.1.3 Nastavení - uživatel jako lokální Admin 47
7.1.4 Nastavení přesměrování tiskáren na terminál 47
7.1.5 Nastavení přesměrování dokumentů 48
ZÁVĚR 51
SEZNAM POUŽITÉ LITERATURY 52
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 53
SEZNAM OBRÁZKŮ 55
SEZNAM TABULEK 56

ÚVOD

Pokud kdokoliv pracuje jako administrátor sítě systému Windows, jeho úspěch z dlouhodobého hlediska velmi závisí na tom, jak v oblasti permanentně se měnících IT technologií, porozumí a ovládne službu Active Directory obsaženou v systému Windows Server. Active Directory je adresářová služba, která je rozšiřitelná a zároveň umožňuje centralizovat správu síťových prostředků. Umožňuje rychlou a snadnou manipulaci s účty pro uživatele, skupinami, počítači a tiskárnami, stejně jako i s dalšími typy prostředků. Téměř jakákoliv úloha související se správou systému Windows, která je provedena, různým způsobem souvisí se službou Active Directory.

Služba Active Directory je v principu založena na standardních internetových protokolech a podrobný návrh zcela přesně a jasně identifikuje fyzické a logické součásti struktury firemní sítě v systému Windows.

Další velmi důležitá věc, kterou by měl administrátor systému Windows velmi dobře ovládat, je nastavování Zásad skupin (Group Policy). Je to zjednodušeně řečeno sada předvoleb a nastavení, které je možno aplikovat na uživatele nebo počítač. A tady již vidíme i souvislost s Active Directory a možností aplikace těchto zásad na různé skupiny uživatelů nebo počítačů ve firemní struktuře. Zásady skupin (Group Policy) zjednodušují administraci stále se opakujících úkonů, které při ručním zavádění okrádají administrátora o drahocenný čas. Může to být třeba instalace nového software na klienty v síti, nastavení mapování svazků souborového serveru, nastavení plochy, Internetového prohlížeče, tiskárny, ale i využití Zásad skupin (Group Policy) k restrikcím na jednotlivých PC stanicích, jako je např. zákaz USB portů, přístupu na Internet, instalace nepovoleného software a jiné.

Zásady skupin (Group Policy) je zjednodušeně řečeno obsáhlý balík pravidel, který může umožnit řízenou konfiguraci operačního systému Windows s návazností na jeho komponenty. Může pomoci při konfiguraci počítače, skriptů uživatele, přesměrování různých adresářů, bezpečnosti počítače, instalací různého software a k mnoha dalším účelům v prostředí jakékoliv firmy nebo podniku.

I. TEORETICKÁ ČÁST

1 MICROSOFT WINDOWS SERVER 2012

Příchod nového systému Windows Serveru 2012 znamená velký krok kupředu, co se týká úplně nových vlastností nebo mnoha dalších vylepšení. Systém Windows Server 2012 v srdci vize operačního systému Microsoft Cloud OS firmám přináší možnosti, které dovede nabídnout pouze společnost Microsoft. Poskytne tím firemní infrastruktuře globální cloudové služby s novými a vylepšenými funkcemi, a to v oblastech virtualizace, správy, úložiště, sítě, infrastruktury virtuálních klientských počítačů, přístupu a ochraně informací, webové a aplikační platformy a mnoho dalšího.

Nový systém Windows Server 2012 znamená pro firemní infrastrukturu vylepšený výkon a rozsah tak, že je možné spouštět i nejnáročnější úlohy, a přitom zároveň poskytuje komplexní možnosti obnovy zajišťující ochranu proti výpadkům.

Díky velmi dobře vylepšené podpoře otevřených rozhraní se mohou flexibilně vytvářet, nasazovat a škálovat aplikace a webové stránky. Toho je dosaženo umožněním přenosu aplikace mezi prostředími a veřejným cloudem či cloudem poskytovatele služeb.

Další novinka je zaměřena na uživatele. Pokud se ve firmě nasadí infrastruktura klientských počítačů (VDI – VIRTUAL DESKTOP INFRASTRUCTURE), tím se výrazně sníží náklady na ukládání dat a to díky širokým možnostem úložiště a deduplikací virtuálních pevných disků (VHD). [1]

1.1 Co je nového ve Windows Server 2012 R2

Již s velkou netrpělivostí byla očekávána nová verze Microsoft Windows Server 2012 R2, ale i jeho dalších edicí. Stále větší nároky na aplikace a síťovou infrastrukturu volaly po výkonnějším a vylepšeném systému Windows Server od Microsoftu. Zde jsou hlavní vylepšení tohoto systému:

Virtualizace serverů – technologie Hyper-V umožňuje spuštění několika operačních systémů, a to včetně systému Windows, Linux a dalších, na jediném serveru. Systém Windows Server 2012 R2 navíc rozšiřuje možnosti technologie Hyper-V o další funkce a špičkovou škálovatelnost pro hostitelské procesory a paměť. [1]

Úložiště – ať jsou platformy firemního úložiště dat jakákoliv, představují uložená dat pro firmu základ veškerého podnikání. Systém Windows Server 2012 R2 pomáhá firmám s optimalizací existujících investic do uložišť dat, jako je síť SAN (Storage Area Network),

což je dedikovaná (oddělená LAN, WAN, atd.) datová síť, která pak slouží pro připojení externích zařízení k serverům, jako jsou disková pole, páskové knihovny a jiná zařízení. Vznik SAN byl hlavně pro potřebu zabezpečení a konsolidaci dat. Systém Windows Server 2012 R2 pomáhá zajistit, aby bylo firemní uložiště vždy k dispozici, a spolu s ním byly k dispozici také všechny služby. [1]

Sítě – společně s nástrojem Systém Center 2012 R2 dokáže systém Windows Server 2012 R2 poskytovat softwarově definované řešení sítí napříč implementacemi veřejného, privátního a hybridního cloudu. To znamená, že celou síť lze velmi dobře spravovat jako jeden server, takže firma při nižších nákladech získá spolehlivost a škálovatelnost několika serverů. Díky funkci automatického přesměrování okolo poruch úložiště, serveru a sítě jsou souborové služby k dispozici online pouze s minimálními výpadky. [1]

Správa serverů a automatizace – rozhraní Windows Management Framework, které využívá přístup správy založené na standardech, poskytuje společnou platformu pro automatizaci a integraci, jež pomocí nástrojů, jako je PowerShell, pomůže zautomatizovat rutinní úlohy. Další vylepšení přispívají ke zjednodušení nasazení, zajišťují správnou konfiguraci datových center a tím umožňují správu napříč více servery prostřednictvím jediného řídícího panelu v nástroji Server Manager. [1]

Webová a aplikační platforma – systém Windows Server 2012 R2 staví své základy na tradici řady systémů Windows Server jakožto mnoha lety prověřené aplikační platformy, pro kterou již byly vytvořeny a nasazeny tisíce aplikací a pro kterou existuje velká komunita čítající miliony zasvěcených a zkušených vývojářů. Aplikace se mohou vyvíjet a nasazovat buď lokálně, nebo v cloudu – využít však lze i obou možností najednou díky hybridním řešením, které fungují v obou prostředích. [1]

Ochrana informací a přístupu – s řešením Access and Information Protection od společnosti Microsoft je možnost spravovat jedinou identitu pro každého uživatele napříč firemními lokálními a cloudovými (SaaS – Software as a Service). Pro vysvětlení se touto zkratkou označují aplikace (v drtivé většině webové), které si firma (uživatel) pronajímá jako službu. Za tuto výhodu samozřejmě platí každý měsíc malý poplatek. V České republice jsou typickou SaaS aplikací třeba e-shop aplikace jako ShopTet, Simplia a jiné. [1]

Infrastruktura virtuálních klientských počítačů – právě se systémem Windows Server 2012 R2 je snadnější nasazovat a zřizovat virtuální prostředky napříč různými zařízeními. Technologie infrastruktury virtuálních klientských počítačů (VDI) nabízí snadný přístup

k uživatelsky přívětivému prostředí systému Windows spuštěnému v datovém centru a to prakticky z jakéhokoliv zařízení. Pomocí technologie Hyper-V a služeb pro vzdálenou plochu nabízí společnost Microsoft tři flexibilní volby nasazení VDI v jediném prostředí: sdružený fond počítačů, osobní počítač a relace vzdálené plochy. [1]

Management Console (GPMC) – nové funkce v systému Windows Server 2012 R2 jsou uvedeny v následujícím obrázku. [1]

Funkce/funkce	Nové nebo aktualizované
Aktualizace zásad skupiny dálkové	Nové
Vylepšení zpráva výsledky zásad skupiny	Aktualizováno
Stav infrastruktury zásad skupiny	Nové
Místní skupiny politiky podpora pro Windows RT	Nové
Optimalizace přihlášení	Aktualizováno
Rychlé spuštění	Nové
Nová skupina politika starter GPO	Nové
Změny rutiny zásad skupiny	Aktualizováno
Registry.pol změny	Aktualizováno
Skupiny klienta zásad služby nečinnosti	Aktualizováno
Nastavení zásad skupiny v Internet Explorer 10	Nové
Předvolby zásad skupiny pro aplikaci Internet Explorer 10	Nové

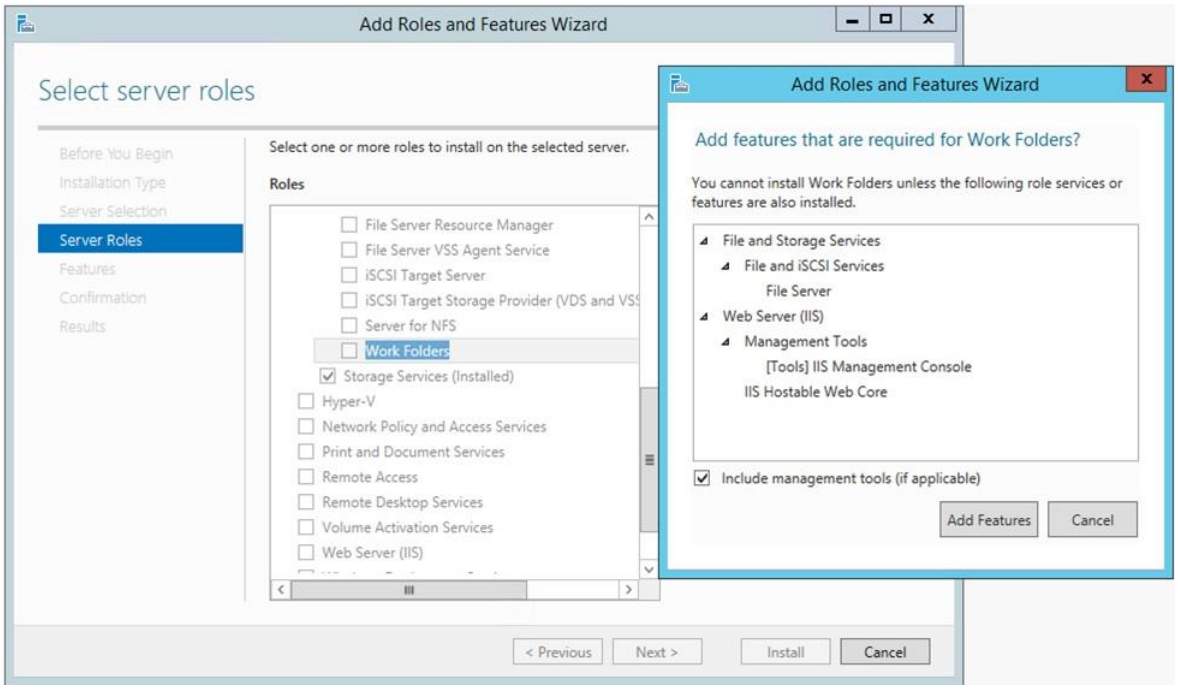
Obr. 1. Nové funkce v systému Windows Server 2012 R2 [1]

Active Directory – v dnešní době chtějí uživatelé jednoduše využívat přístup k firemním aplikacím odkudkoliv a z jakéhokoliv mobilního zařízení. Zároveň potřebují mít vždy aktuální verzi dokumentu, který je uložen na sdíleném disku v práci. Systém Windows Server 2012 R2 přináší v této oblasti hodně novinek. [1]

Workplace Join **–** s touto technologií mohou uživatelé využít jejich zařízení (BYOD - Což doslova znamená: "Přineste si své vlastní zařízení.") pro přístup k firemním datům. Během registrace zařízení do firemní sítě je v Active Directory vytvořen objekt pro nové zařízení, a na zařízení je následně nainstalován certifikát. Pro přístup k firemním zdrojům pak lze využít dvoufaktorovou autentizaci. [2]

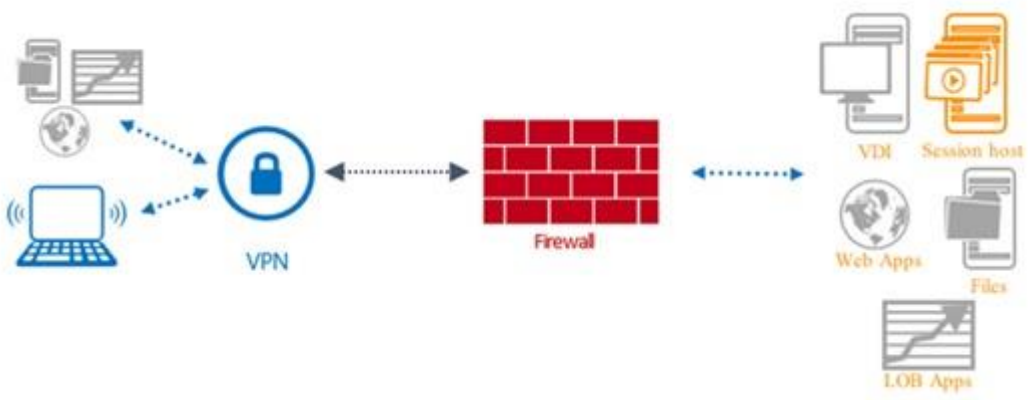
Workfolders **–** jedná se o novou funkcionalitu v oblasti File Services, která umožňuje synchronizaci firemních dat uložených na souborovém serveru do zařízení uživatele.

Výhodou je integrace s Active Directory Rights Management Services, která chrání data proti zneužití. [2]



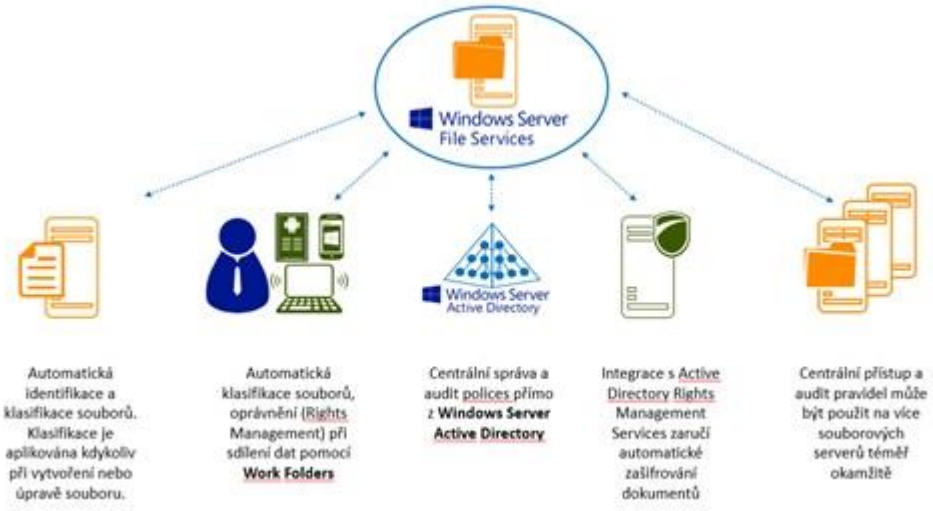
Obr. 2. Přidávání Server Roles v Microsoft Server 2012 R2 [2]

Automatic VPN connections **–** automatické vytočení VPN připojení na základě požadavku aplikace. VPN připojení se automaticky naváže, kdykoliv si aplikace vyžádá přístup k firemním zdrojům. Uživatelům i nadále zůstává ověření pomocí dvoufaktorové autentizace. [2]



Obr. 3. Schéma - Automatic VPN Connections ve Windows Server 2012 R2 [2]

Dynamic Access Control – tato funkcionalita byla poprvé představena ve Windows Serveru 2012. Jedná se o komplexní ochranu a klasifikaci citlivých dat s využitím technologií Active Directory, File Server Resource Manager (AD RMS). Data uložená na souborovém serveru se mohou klasifikovat na základě jejich obsahu, umístění a dalších kritérií. Klasifikovaná dat mohou být dále použita pro audit informací, kontrolu přístupů a automatickou klasifikaci souborů. Dynamic Access Control využívá pro ochranu citlivých informací technologii Active Directory Rights Management Services (AD RMS). [2]



Obr. 4. Schéma pro Dynamic Access Control [2]

2 ACTIVE DIRECTORY

2.1 Služba Active Directory

Active Directory je vlastně adresářová služba, která je součástí systému Windows Server. Tato služba zahrnuje adresář (Directory) a to je vlastně databáze s hierarchickou strukturou), ve kterém jsou uloženy informace o distribuovaných prostředcích, o službách, prostřednictvím nich jsou tyto informace užitečné a lehce dostupné. Adresář se však liší od klasické relační databáze. Je totiž navržen tak, aby vyhovoval častému čtení, vyhledávání a jen k občasnému záznamu. Přístup k záznamům můžeme libovolně omezovat pomocí ACL (Access Control List).

V podstatě všechny verze systému Windows Server a to začátkem systému Windows 2000 podporují službu Active Directory. [3]

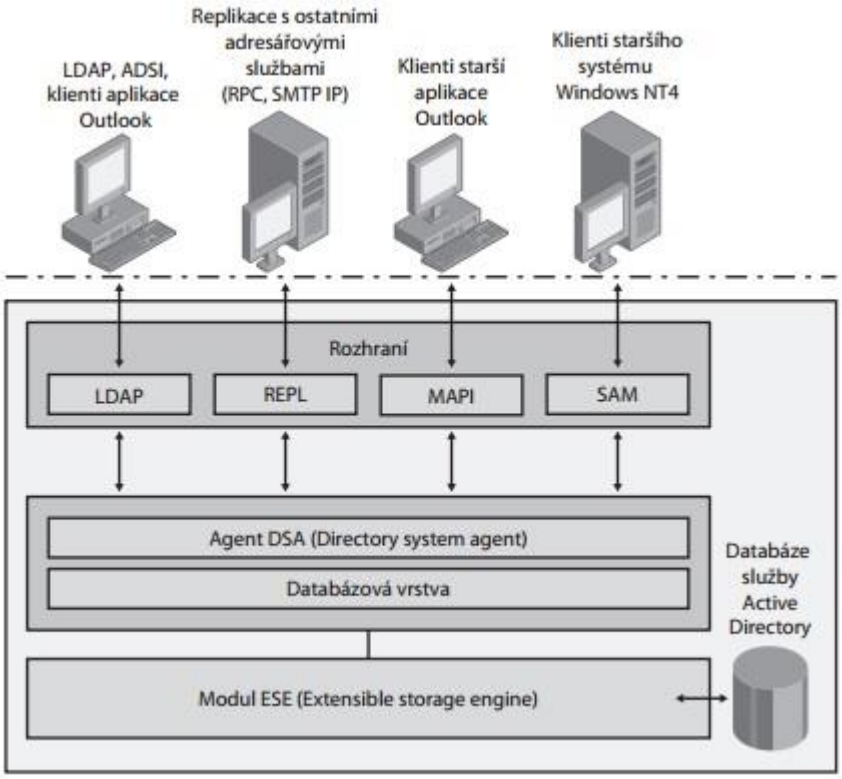
2.2 Doménové služby Active Directory

Domény systému Windows, které využívající službu Active Directory, se nazývají domény služby Active Directory. Data (informace o pojmenovaných objektech v síti organizačně sdružené do skupin) jsou uložena v jediném distribuovaném úložišti a tím jeho údržba nevyžaduje tak velký rozsah správy, při současném, velmi snadném přístupu z různých umístěních v síti.

Právě využitím fyzických a logických struktur, které poskytuje služba Active Directory, lze měnit velikost adresáře (databáze s hierarchickou strukturou) tak, aby nejlépe splňoval požadavky růstu firmy nebo podniku. [3]

2.2.1 Rozhraní služby Active Directory

Služba Active Directory je navržena takovým způsobem, aby vzájemně spolupracovala s jinými adresářovými službami a zároveň akceptovala různé požadavky od mnoha klientů, kteří využívají různá rozhraní. [3]



Obr. 5. Služba Active Directory a její spolupráce s jinými klienty [3]

Protokol LDAP verze 3 (Lighweight Directory Access Protocol) je vlastně primárním protokolem Active Directory. Je to v podstatě aplikační protokol pro dotazování a samozřejmě i modifikaci adresářových služeb nad protokolem TCP/IP. Přibližně v 80. letech minulého století vznikla skupina standardů X.500 (DAP, DSP, DISP, DOP) protokolů, jenž pokryly adresářové služby. A právě zjednodušením standardu X.500 a nasměrováním na protokol TCP/IP vznikl protokol LDAP. [4]

Samotný protokol LDAP používá LDAP DATA Interchange Format (LDIF), což je vlastně standardizovaný textový formát, který slouží pro výměnu dat. [4]

Data jsou sice při přenosu kódována a to pomocí Lightweight Encoding Rules (LBER), ale toto kódování není z důvodu nějaké bezpečnosti, ale pouze z důvodu nehomogenity prostředí, proto se dají data lehce dekódovat. LDAP lze popsat pomocí čtyř modelů: [4]

- informační model
- jmenný model
- funkční model
- bezpečnostní model

Informační model

Informace je uložena ve stromové struktuře a označuje se jako Directory Information Tree (DIT). RootDSE je zároveň kořenem adresářového stromu a obsahuje celkové informace o adresáři, ale nemá žádné jméno a třídu. Informační model je vlastně založen na záznamech s obsahem informace o nějakém konkrétním objektu. Může to být třeba uživatel nebo počítač. Vlastní implementaci Informačního modelu označujeme jako schéma, které představuje sadu objektů definujících strukturu i obsah každého objektu, který lze vytvořit v adresářové službě. Pomocí schéma definujeme úplně všechny možné třídy objektů a zároveň atributy. Výchozí schémata určitého adresáře nejsou konečné a lze je třeba rozšiřovat a příkladem může být Microsoft Exchange Server v Active Directory. Tím se např. schéma rozšíří atributy pro poštovní služby. [4]

Třídy objektů (Object Classes) označují kategorie objektů, které v adresáři mohou být vytvořeny. LDAP používá označení „objectClass“ a to může být např. user, domain, container, group, computer. Třídy objektů jsou řazeny do tří kategorií Structural, Abstract a Auxiliary. To ale znamená, že objekt může být zařazen do více tříd současně. Například uživatel (user) v AD je zařazen ve třídě person, top, organizationalPerson a user a v těchto třídách může být zařazen i computer, ale má navíc ještě zařazení do třídy computer.

Aby bylo hledání přesné a efektivní, musíme použít hledání podle atributu objectCategory, který na rozdíl od objectClass pouze jednu hodnotu, což vede na odkaz nejvíce specifikované třídy v hierarchii tříd objektů. [4]

Atributy objektů (Object Attributes) značí charakteristiky objektů. Atribut může obsahovat i více než jednu hodnotu (např. jméno, příjmení, mail). Určité atributy patří jen k určité třídě objektů. Které hodnoty musí být vyplněny a které jsou volitelné, nám definuje schéma. Schéma také určuje, jakých hodnot nabývá atribut, např. textový řetězec, celé číslo a další.

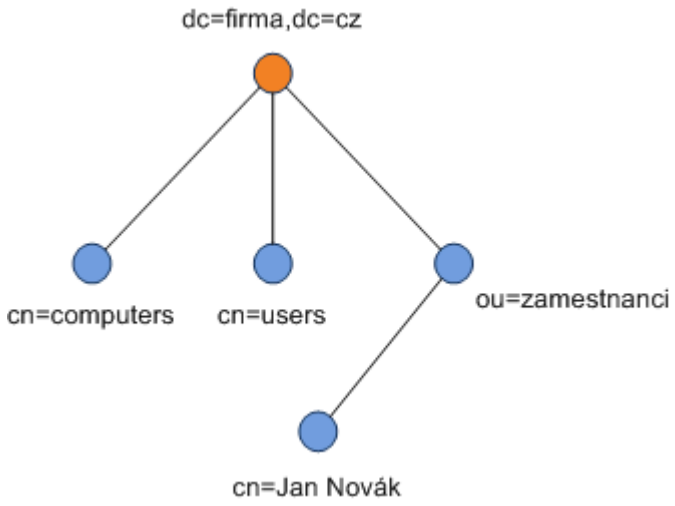
Podle umístění ve stromové struktuře, se může jednat o list (Leaf Object) bez potomků, nebo kontejner (Container Object) a ten může obsahovat více objektů. Následující obrázek ukazuje několik běžných atributů používaných v Active Directory: [4]

jméno	popis
sAMAccountName	SAM Account Name, přihlašovací uživatelské jméno, které podporuje starší systémy
sAMAccountType	typ účtu
userPrincipalName	UPN, přihlašovací jméno uživatelského účtu ve tvaru <user>@<DNS-domain-name>
displayName	jméno, které využívají aplikace (třeba Exchange)
givenName	křestní jméno
sn	surname – příjmení
description	popis
mail	adresa elektronické pošty
company	jméno společnosti
department	oddělení ve firmě
location	umístění
streetAddress	ulice
memberOf	seznam skupin, kterých je členem

Obr. 6. Běžné atributy používané v Active Directory [4]

Jmenný model

Jmennný model (Distinguished Name – DN) se používá pro identifikaci objektů. Je to vlastně jednoznačný identifikátor objektu s úplnou cestou záznamu (pozice ve stromu). DN je složen ze jména objektu a jmen jednotlivých kontejnerů i domén, které obsahují objekt, a ten je oddělen čárkou. Pod jednotlivými položkami jsou názvy atributu s jeho hodnotou, např. ou=zamestnanci. Obrázek ukazuje část adresáře Active Directory pro doménu firma.cz. [4]



Obr. 7. Část adresáře Active Directory [4]

Když nechceme specifikovat úplnou cestu k objektu, tak se dá použít Relative Distinguished Name (RDN) a to je relativní a zároveň jednoznačné v daném kontejneru (RDN = cn=Jméno Příjmení).

Pro identifikaci objektu lze však použít i OID (Object Identifieres). Jedná se o hierarchický, unikátní identifikátor, který se skládá z dekadických číslic oddělených tečkou. Je to stejný identifikátor jako u protokolu SNMP a je běžný u X.500.

V Active Directory má každý objekt přiřazeno 128-bitovým číslo (GUID – Globally unique identifier), které je unikátní a jednoznačné. Číslo je neměnné při přesunu v rámci lesa.

Active Directory používá i obdobu DN a nazýváme ji jako AD Canonical Name. Příkladem může být zápis: firma.cz/zamestnanci/Jméno Příjmení.

Každá část DN se vyjadřuje pomocí typ atributu=hodnota. Tento typ atributu, který se používá k RDN popisu, označujeme *jmenný atribut.* Každá třída má jmenný atribut (např. User má *cn.* V následujícím obrázku je ukázka jmenných atributů a ekvivalentů pro Active Directory.

LDAP atribut	jméno	AD atribut	jméno
CN	Common Name	CN	Common Name
OU	Organization Unit	OU	Organization Unit
O	Organization	DC	Domain Component
C	Country	-	-

Obr. 8. Jmenné atributy a ekvivalenty pro AD [4]

Funkční model

Funkční model pro LDAP definuje, co všechno se provádí s informacemi v adresáři.

Je to devět operací zařazených ve třech funkčních oblastech. [4]

oblast	operace	popis
autentizace (Authentication)	bind	inicializuje spojení, vyjednává o metodě autentizace, autentizuje
	unbind	ukončí session
	abandon	klient žádá o ukončení posílání výsledků na poslední dotaz
dotazování (Interrogation)	search	výběr dat z určitého regionu pomocí filtru
	compare	porovná hodnotu atributu se zadanou hodnotou
aktualizace (Update)	add	vytvoří nový objekt
	modify	upraví atributy záznamu (vytvořit, smazat, upravit)
	modify RDN	slouží k přesunutí objektu v rámci stromu adresáře
	delete	smazání záznamu

Obr. 9. Operace LDAPu [4]

Active Directory podporuje i několik dalších operací. Ty však nejsou definovány v RFC (Request for Comments). Např. operace search disponuje řadou vstupních parametrů. Třeba *výchozí bod hledání* určuje kontejner, od kterého níže se bude začínat prohledávat. Ve filtru (jeden z důležitých parametrů) se dají použít matematické operace např. shoda, větší než, menší než a přibližná hodnota. Filtry se dají kombinovat s logickými operacemi např. AND, OR a NOT. Výhodou je i použití zástupného znaku * pro libovolný znak.

Vyhledávání pomocí filtrů:

```
(objectCategory=*)                          // všechny objekty
(&(objectClass=user) ( ! (cn=Susan)))       // všichni uživatelé mimo Susan [4]
```

Bezpečnostní model

Tento poslední model LDAP, určuje přístup k datům z bezpečnostního hlediska. [4]

3 CO JE GROUP POLICY – SKUPINY ZÁSAD VE WINDOWS

Skupiny zásad (Group Policy) je důležitý nástroj pro hromadnou správu různých oprávnění a nastavení aplikovaných jak na celý počítač, tak na uživatele, který je přihlášen. Právě ve skupinách zásad je možné vytvářet mnoho kolekcí nastavení, kterým říkáme Group Policy Object GPO, které dovedou měnit konkrétní parametry chování počítače tak i uživatele. Samotné nastavení GPO se pak „linkuje“ na jednotlivé organizační jednotky OU předem vytvořené v AD (Active Directory). Tím se zajistí aplikování určitých nastavení jen na vybrané počítače nebo uživatele. [5]

3.1 Pro co se Group Policy používá

Group Policy jako nástroj pro hromadnou správu oprávnění a nastavení aplikovaných jak na celý počítač, tak na přihlášeného uživatele se používá pro:

- aplikování firemních standardů (skrytí ovládacích panelů, síťové tiskárny, spouštění scriptů)
- aplikování zabezpečení (změna oprávnění na určitých složkách, složitost hesla, skupiny s možností se lokálně přihlásit)
- hromadná instalace aplikací (Office, Adobe Reader, a jiné.) [5]

3.2 Group Policy Object “GPO“

Je to seskupení několika nastavení najednou:

- komponenta globální politiky
- dělí se na nastavení pro počítač tak i na nastavení pro uživatele
- zásady nastavení pro počítače se vztahují jen na počítače a ukládají se v rámci objektů GPO do uzlu Konfigurace počítače (Computer Configuration)
- zásady nastavení pro uživatele se vztahují jen na uživatele a ukládají se v rámci GPO objektů do uzlu Konfigurace uživatele (User Configuration)
- linkují se na organizační jednotky OU v AD (Active Directory)
- jeden GPO může být linkován i na několik OU [5]

3.3 Dělení Policy “Politiky “’

Politiky dělíme na Lokální (Local Group Policy) a Doménové (Domain Group Policy)

3.3.1 Lokální politiky (Local Group Policy LGPO)

Každý počítač již od Windows 2000 má lokální politiky (Local Group Policy), které ovlivňují lokální počítač a přihlášené uživatele na něj. Pokud není počítač připojen do domény, tak právě tyto lokální politiky jsou použity jako jediné. Pokud například vytvořím uživatele na počítači a nastavím mu nějaké omezené oprávnění, chování právě tohoto uživatele vymezuje lokální politika. Tyto lokální politiky jsou uloženy ve skrytém adresáři %systemroot%\system32\GroupPolicy. [5]

Počítače od operačního systému Windows Vista a novější již připouštějí více objektů LGPO a to na jednom počítači (samozřejmě pokud tento počítač není řadičem domény). Na počítačích, které to umožňují, potom existují tři stupně objektů LGPO: [5]

Místní objekt zásad skupin – tento místní objekt LGPO je na samém vrcholu hierarchie zásad skupiny pro místní počítač. Tento objekt LGPO je jako jediný objekt LGPO na lokálním počítači, který dovoluje aplikaci konfigurace počítač i zároveň konfiguraci uživatel na všechny uživatelské účty na tomto počítači. [5]

Administrátorský objekt LGPO / Neadministrátorský objekt LGPO – to jestli se uplatní administrátorský nebo neadministrátorský objekt LGPO, to je závislé na tom, jaký uživatelský účet je aktivní. Pokud je účet členem skupiny Administrators na lokálním počítači, pak s použije administrátorský LGPO. V opačném případě je to neadministrátorský LGPO. Důležité je upozornit, že v tomto objektu jsou obsažena pouze nastavení pro konfiguraci uživatele. [5]

Uživatelský objekt LGPO – uživatelské objekty LGPO se vztahují pouze k vybranému uživatelskému účtu nebo skupině. Tento objekt obsahuje také pouze konfigurace uživatele. [5]

Jako první je zpracován místní objekt LGPO, potom je zpracován administrátorský nebo neadministrátorský objekt LGPO, a jako poslední uživatelský objekt LGPO.
Použití LGPO má opravdu jen význam pro počítače mimo doménu. Pokud jsou počítače v doméně a je aktivní Active Directory, tím má již většina počítačů a uživatelů aplikováno více objektů GPO, a zavedení dalších místních objektů LGPO k tomuto množství objektů GPO již může být matoucí a mohou nastat zbytečné konflikty. Proto se doporučuje pro počítače v doméně používat pouze doménových GPO a zpracování místních objektů LGPO zcela vyloučit. To se provede pomocí zásad skupiny. Na počítačích od Windows

Vista a novějších se potlačí zpracování místních objektů LGPO tak že se povolí nastavení Vypnout zpracování místních objektů Zásad skupiny (Turn Off Local Group Policy Objects Processing) v nějakém objektu GPO, který se aplikuje na daném počítači. [5]

Pokud jsou aktivní jak doménové tak místní zásady, uplatňují se v následujícím pořadí:

- Místní objekty LGPO
- Objekty GPO pro lokalitu
- Objekty GPO pro doménu
- Objekty GPO pro organizační jednotku
- Objekty GPO pro podřízenou organizační jednotku [5]

Aplikování politik je potom z úrovně 1 na úroveň 5. Pokud tedy na úrovni jedna je nastaveno např. PROXY Enable a na úrovni 4 je PROXY Disable, vyhraje úroveň 4 a nastavení proxy zůstane ve stavu Disable.

3.3.2 Doménové Politiky

Doménové politiky lze použít výhradně u počítačů a uživatelů, kteří jsou členy nějaké domény. Po založení nové domény i jejího řadiče jsou potom automaticky vytvořeny dva objekty GPO: [5]

Objekt Default Domain Policy je objekt GPO vytvořený k účelu propojení s celou doménou v Active Directory. Toto propojení je provedeno automaticky. Tento objekt GPO je používán k výběru základních nastavení zásad, která se uplatňují na všechny uživatele a počítače v doméně. [5]

Objekt Default Domain Controllers Policy je objekt GPO, který je automaticky vytvořený a propojený s organizační jednotkou Domain Controllers, která se vztahuje na všechny doménové řadiče dané domény (do té doby dokud nejsou odstraněny z této organizační jednotky). Tento objekt se většinou používá k ovládání bezpečnostních nastavení pro řadiče v doméně. [5]

Oba tyto výchozí objekty GPO jsou pro správné fungování a zpracování zásad skupiny nepostradatelné. Standardně má vždy objekt GPO Default Domain Policy přednost před všemi ostatními objekty propojenými s doménou. Objekt Default Domain Controllers Policy má obdobně přednost před všemi ostatními objekty GPO propojenými s organizační jednotkou Domain Controllers. [5]

3.4 Hlavní využití objektu Default Domain Policy

Velmi obvyklou praxí je, že se v objektu Default Domain Policy provádí jen úpravy výchozích nastavení zásad účtů (Account policies) a ještě tři specifické oblasti týkající se uživatelských účtů:

- Zásady hesla (Password policy) – určuje výchozí zásady hesel pro doménové řadiče, např. jako je stáří hesel a minimální délka.
- Zásady uzamčení účtů (Account lockout policy) – zde se stanovují výchozí zásady pro uzamčení účtů, jako jsou doba uzamčení účtu a prahová hodnota pro uzamčení účtu.
- Zásady modulu Kerberos (Kerberos Policy) – zde se definují výchozí zásady modulu Kerberos pro doménové řadiče, např. maximální tolerance synchronizace hodin počítače. [5]

Při změně jiných oblastí zásad, by se měl nejdříve vytvořit nový objekt GPO a ten propojit s doménou nebo určitou organizační jednotkou v doméně. Přesto je však několik výjimek při nastavování zásad, kdy není třeba vytvářet nový objekt GPO a lze využít Default Domain Policy (např. Přejmenovat účet správce, Stav účtu správce, Vynutit odhlášení, pokud vyprší časový limit pro přihlášení). [5]

3.5 Ovlivnění aplikování GPO politik

Samotné aplikování GPO politik je možné ovlivňovat, a to přímo na úrovni každé konkrétní z politik (GPO). Z toho vyplývá, že na každé politice může být nastaveno: [5]

Method	Description
Blocking inheritance	Blokování dědění doménových politik nebo politik z nadřazených OU
Enforcement of GPO links	Vynucení politiky. Využívá se, pokud chcete zajistit, že politika nebude přepsána.
Filtering using security groups	Na Každé GPO je možné nastavit oprávnění, tím můžete definovat, na jaké uživatele či skupiny bude politika aplikována
Filtering using WMI filters	Pomocí WMI filtrů je možné aplikování politik, třeba jen na PC s WIN XP, nebo na počítače s větší RAM od 3GB atd.
Disabling GPOs	Můžete zcela zablokovat použití GPO pro danou síť, doménu nebo organizační jednotku. Můžete také zcela vypnout část GPO Uživatele nebo Počítače, aby výsledná politika měla menší velikost

Obr. 10. Možné nastavení na každé politice GPO [5]

3.6 Dědičnost zásad skupin

Když se vytváří a upravují objekty zásad skupin GPO, nastavení a předvolby zásad, které používáme, ovlivňují konfiguraci počítačů a uživatelů. [5]

Prostřednictvím dědičnosti se objekt GPO aplikovaný přímo na rodičovský kontejner přenáší také na podřízený kontejner. Předvolby a nastavení zásad v tomto objektu GPO se předávají z jednoho objektu Active Directory a to na objekt, který je postavený v hierarchii pod ním. Potom díky dědičnosti se každý objekt typu počítač nebo uživatel, který je součástí určité domény, ať je uložen v jakémkoli kontejneru, stává předmětem zpracování zásad skupin. [5]

Naprostá většina zásad se může nacházet v jednom ze tří stavů:

- Nedefinováno (Not Configured)
- Povoleno (Enabled)
- Zakázáno (Disabled) [5]

Pro většinu nastavení je výchozí stav Nedefinováno (Not Configured). Je-li nějaké nastavení zásad povoleno, bude potom nastavení této konfigurační možnosti vynuceno a aplikováno na všechny uživatele i počítače, které jsou předmětem této zásady, a to buď přímo, nebo prostřednictvím dědičnosti. [5]

Předvolby zásad nabývají ve většině případů těchto čtyř stavů:

- Vytvořit (Create) – Vytvoří předvolbu, pokud neexistuje.
- Nahradit (Replace) – Pokud předvolba existuje, tak je smazána a znovu vytvořena.
- Aktualizovat (Update) – Mění parametry existující předvolby, nebo ji vytvoří, pokud neexistuje
- Odstranit (Delete) – Vymaže předvolbu bez náhrady. [5]

Fungování dědičnosti se dá ovlivnit čtyřmi způsoby:

- Změna pořadí propojení a tím i jejich priorit.
- Potlačení dědičnosti (pokud není dědičnost vynucena).
- Blokování dědičnosti (zabrání dědičnosti zcela).
- Vynucení dědičnosti k zamezení, potlačení a blokování dědičnosti. [5]

3.6.1 Změna pořadí propojení a priorita

Dědičnost začíná v systému zásad skupiny vždy na úrovni lokality, potom prochází přes domény až na úroveň organizačních jednotek. Pokud je však na stejné úrovni propojeno více objektů GPO, záleží na pořadí jejich propojení, jak budou jednotlivé objekty aplikovány. Propojené objekty zásad jsou vždy aplikovány v pořadí podle jejich propojení.

Objekty s vyšším pořadovým číslem propojení, umístěné v seznamu níže, jsou vždy zpracovány před těmi, které mají nižší pořadové číslo propojení a jsou umístěny výše. [5]

3.7 Globální politiky a rozdělení GPO

Globální politiky se dělí na dvě části. Na konfiguraci počítače (Computer Configuration) a konfiguraci uživatele (User Configuration)

- konfigurace počítače mění registry v : HKEY_LOCAL_MACHINE
- konfigurace uživatele mění registry v : HKEY_CURRENT_USER [6]

Při tvoření GPO je možnost jednu z částí (Uživatel/Počítač) vypnout a tím snížit celkovou velikost už vytvořené GPO. [6]

Konfigurace počítače i uživatele se ještě dělí na další tři sekce:

- nastavení software (Software settings) – Instalace software. Pokud je definován v části konfigurace počítače, bude nainstalován ještě před přihlášením, pokud je definován v části konfigurace uživatele, bude nainstalován až po přihlášení konkrétního uživatele.
- nastavení systému Windows (Windows settings) – Obsahují skripty (při přihlášení, při odhlášení) a nastavení zabezpečení pro uživatele a zároveň počítače. Další nastavení je zabezpečení pro Internet Explorer
- šablony pro správu (Administrative templates) – Obsahují stovky nastavení registru pro ovládání nejrůznějších aspektů uživatele nebo počítačového prostředí. [6]

Aplikování Skupin zásad se děje na dvou úrovních a to zvlášť pro konfiguraci počítače a zvlášť pro konfiguraci uživatele. Toto aplikování zajišťuje služba Group Policy Client. [6]

3.8 Způsob aplikování GPC (Group Policy Client)

Aplikování konfigurace počítače:

- při startu počítače, nebo každých 90 minut (pozn. Aplikování konfigurace počítače každých 90min, je až od operačního systému Windows Vista. Na operační systém Windows XP se aplikovaly pouze při spuštění počítače.)
- aplikují se Startup skripty (startovací skripty) [6]

Aplikování konfigurace uživatele:

- při přihlášení (zalogování) uživatele a jinak každých 90 minut
- aplikují se přihlašovací skripty (Logon skripty) [6]

3.8.1 Jak se GPO zpracovává při spuštění počítače a přihlášení uživatele

1. Počítač najde DC a přihlásí se k němu, stejně jako uživatel. Pro úspěšné přihlášení musí být povolené porty: UDP 53 (DNS), UDP a TCP 389 (LDAP), TCP 135 (RPC Portmapper), UDP 88 (Kerbedos).
2. Počítač pomocí ICMP paketů zjistí, zda je na pomalé lince (Slow Link Detection).
3. Pomocí LDAPu zjistí jaké GPO jsou navázány na OU, doménu a síť. Z těchto odpovědí si vytvoří seznam všech GPO které jsou na něj aplikovány.
4. Pomocí LDAPu pošle počítač dotaz na seznam filtrů všech GPO, které našel. Dále si požádá o atributy jako je cesta ke GPT (Group Policy Templates), číslo verze GPC (Group Policy Configuration), gpCMachineExtensionNames a gpCUserExtensionnames attribut.
5. Počítač pomocí protokolu SMB (Server Message Block – port TCP 445) se připojí k SYSVOLu a přečte si GPT.INI pro každé GPO, které se na něj aplikuje.
6. Group Policy proces začne porovnávat verzi GPO s Verzí GPO, kterou má lokálně uloženou v registru: (HKEY_LOKAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Group Policy\History).
7. Pokud se verze GPO nezměnila, tak je přeskočena. V GPO se ale dá nastavit, aby se toto nedělo a politiky se aplikovaly pokaždé, i když nenastala změna. Nevýhodou je časová prodleva, která je způsobena opětovným aplikováním všech politik. Opětovné vynucení všech politik se dá provést přes Příkazový řádek (CMD) pomocí příkazu gpupdate /force

8. CSE (Client Side Extension) zjistí, jestli má dostatečná práva na všechny GPO, které se budou aplikovat. Pokud tomu tak není, tak je dané GPO vyhozeno ze seznamu. Pokud je na GPO nastaveno Enforced (vynucené), pak jev tomto kroku přeneseno až na konec seznamu. Z toho vyplývá, že nastavení z tohoto GPO vždycky vyhrávají, pokud by nastal nějaký konflikt.
9. CSE začne postupně zpracovávat jednotlivá GPO.
10. Po každém zpracování GPO CSE zaloguje RSoP (Result of Policy) přes službuWMI (Windows Management Instrumentation) do CIMOM (Common Information Model Object Manager) databáze na počítači, kde se zpracovávají politiky.
11. Po přihlášení se celý proces opakuje s nastavením aplikovaných na uživatele. [6]

3.8.2 Výjimky při aplikování politik GPO

Globální politiky dokáží detekovat rychlost linky počítačové sítě a v případě pomalé linky (méně než 500 kb/s) a několika dalších faktorů, nemusí být některé z politik aplikovány. [6]

V následujícím obrázku jsou příklady některých politik a jejich chování při aplikaci po vyhodnocení pomalé linky počítačové sítě. Také je vyhodnoceno, jestli se tento proces aplikace dá změnit při neúspěšném aplikování díky pomalé lince počítačové sítě.

Procesy	Aplikování při zjištění pomalé linky	Může se dát změnit?
Zpracování zásad registru	Ano	Ne
Nastavení Internet Explorer	Ne	Ano
Politiky instalování SW	Ne	Ano
Politiky přesměrování adresy	Ne	Ano
Scripty	Ne	Ano
Politiky zabezpečení	Ano	Ne
Internet Protocol Security (IPSec)	Ne	Ano
Politiky bezdrátových sítí	Ne	Ano
EFS Recovery	Ano	Ano
Politiky diskových kvót	Ne	Ano

Obr. 11. Možnost změny aplikace GPO při pomalé lince

3.9 Šablony a ADM a ADMX soubory

Z důvodu rozsáhlosti nastavení a možnosti grafického zobrazení v GPM (Group Policy Management) Skupinových zásad vznikly šablony, které v sobě již zahrnují přednastavené vlastnosti GPO podle použití, nebo mohou sloužit k vytváření nových GPO. Od Windows Vista a Serveru 2008 máme již dva formáty a to staré ADM a nové ADMX. [5]

Administrative Templates soubory (ADM a ADMX), obsahují šablony, které dovolují konfigurovat nějakou vlastnost pomocí změn v registrech. Když je vytvářena Group Policy Object (GPO politika) pomocí Group Policy Object Editor (GPOE) či Group Policy Management Console, tedy Group Policy Management Editor (GPME), potom se ADM/ADMX soubory načtou a v editoru se zobrazí určité položky. Když se nějaká položka změní, potom se uvnitř politiky uloží do souboru registry.pol. Ten se pak aplikuje na počítače/uživatele. Šablony jsou ale potřeba jen pro vytváření politiky, ale ne již pro vlastní aplikaci na klientovi. [5]

Základní ADM/ADMX soubory se distribuují spolu s operačním systémem. ADM/ADMX soubory v sobě obsahují nejen nastavení pro aktuální operační systém, ale pro všechny platformy podporované v dané době (to znamená, že na Windows XP máme i informace k serverovým nebo starším operačním systémům). Také i nové defaultní ADMX soubory obsahují vše, co bylo ve standardních ADM souborech. [5]

Na internetu můžeme stáhnout různé rozšiřující ADM/ADMX soubory, například pro Internetové prohlížeče Firefox, Google Chrome nebo MS Office. Případně i ty ADM/ADMX soubory, které jsou součástí různých verzí Windows. Není ani problém si vytvořit vlastní ADM/ADMX soubor s nějakým nastavením. [5]

Soubor ADM - jedná se o původní formát souborů pro šablony od Windows 2000 po 2003/XP. Je to textový soubor, který je jazykově závislý (pro každý jazyk máme nový soubor stejného názvu, tzn. konfigurace politiky lze provádět pouze v jednom jazyce). ADM soubory můžeme použít i v novějších verzích operačního systému (Windows 7), ale standardní soubory, distribuované s operačním systémem, jsou již pouze ADMX a tyto soubory mají vždy přednost před ADM. Pokud ale používáme ADM soubory při vytváření politiky, tak se tyto soubory ukládají do vytvořené politiky (do Sysvol adresáře v doméně). Takže politika již má velikost několik MB místo pár kB. [5]

Soubor ADMX - jedná se vlastně o náhradu ADM souborů, která přišla s Windows Vista a Windows Server 2008. ADMX je soubor v XML formátu, který je jazykově neutrální. K určitému ADMX souboru potřebujeme odpovídající ADML soubor. Tím je podporována multijazyčnost (více správců může editovat jednu politiku, každý v jiném jazyce). ADMX/ADML soubory se navíc neukládají do vlastní politiky, takže ta je výrazně menší. Volitelně můžeme použít Central Store (centrální uložiště). [5]

Soubor ADML - je to vlastně doplněk ADMX souboru, který již obsahuje jazykové informace (texty pro konkrétní politiku v určitém jazyce). Ve složce s ADMX soubory se vytváří podadresáře pro různé jazyky (jako en-US, cs-CZ či de-DE) a do nich se ukládají ADML soubory se stejným názvem jako ADMX. [5]

Načítání ADMX souborů - v administračních nástrojích (GPOE, GPME) se ADMX soubory automaticky hledají ve dvou cestách. V Central Store, tedy síťovém úložišti v doméně, jehož adresa je \\FQDN\SYSVOL\FQDN\policies\PolicyDefinitions. Pokud se zde nenalezne, tak se hledá v lokálním úložišti v c:\Windows\PolicyDefinitions. Pokud Central Store existuje a je dostupný, tak se lokální soubory nepoužijí. [5]

Vytvoření Central Store - Pokud chceme vytvořit Central Store, tak stačí založit daný adresář na jednom doménovém řadiči (provede se replikace na ostatní) a zkopírovat do něj ADMX a ADML soubory například z Windows Server 2008 R2. Vždy je potřeba udržovat nejnovější verzi těchto souborů, aby obsahoval všechna nastavení (například po instalaci Service Pack). V současnosti nejnovější verze je pro Windows Server 2008 R2/Windows 7.

Pokud používáme systém s ADMX soubory, tak můžeme stále přidat ADM soubory, ty se zobrazí pod skupinou Classic Administrative Templates (ADM). [5]

Načítání ADM souborů - naproti tomu ADM soubory jsou standardně (pokud je máme v systému) uloženy v c:\Windows\inf. Při vytváření politiky (ve Windows, kde ještě nejsou ADMX) se načítají některé defaultní a můžeme je ručně přidávat nebo ubírat. Klikneme pravým tlačítkem na Administrative Templates v editoru a zvolíme Add/Remove Templates. Defaultní ADM soubory jsou conf.adm, inetres.adm, system.adm, wmplayer.adm, wuau.adm. Těchto 5 souborů má dohromady téměř 4 MB a vkládají se vždy do každé vytvořené politiky. [5]

Uložení GPO - politiky (GPO) se v každé doméně ukládají (na doménové řadiče) do cesty \\FQDN\SYSVOL\FQDN\policies. Zde je taky adresář pro každou politiku, který má název {GPO GUID} (ID politiky v závorkách). Pokud je to politika, která byla vytvořená pomocí ADM souboru, tak se zde nachází podadresář Adm, který obsahuje všechny ADM soubory, které byly při vytváření postupně přidány. Takže je odsud můžeme i zkopírovat, pokud je potřebujeme. Ale určitě je daleko efektivnější používat nové ADMX soubory uložené v Central Store (jednotlivé politiky jsou pak mnohem menší), to znamená již vytvářet a spravovat politiky v nových verzích Windows. [5]

Převod politiky s ADM soubory na novou - jak bylo řečeno, je lepší vytvářet nové politiky v novějších verzích OS (třeba Windows 7) a v nich provádět i jejich správu (nové položky bychom ve starších OS neviděli a rovnou by se do GPO přidali ADM soubory). Staré politiky můžeme editovat i v nových OS, ale tím se ADM soubory neodstraní (i když pokud nejsou speciální, tak je ani při editaci nevyužijeme – pokud existuje odpovídající ADMX, tak má přednost ten). [5]

Jak se zbavit ADM souborů - čistým řešením, jak se úspěšně zbavit ADM souborů, je vytvořit GPO znovu. Lákala by možnost importovat nastavení ze staré politiky do nové, ale při importu se vloží i ADM soubory. Přesto se někdy i možnost importu může někdy hodit, ta zkopíruje nastavení (a pouze to, ne práva, delegaci apod.) ze zálohované politiky. Zálohu můžeme provést v jednom kroku průvodce. Import se provede pomocí Group Policy Management Console, proklikáním se na Group Policy Objects a kliknutím pravým tlačítkem na politiku, do které se bude importovat nastavení. Změnu lze provést ve volbě Import Settings. Možností, jak odstranit ADM soubory z existující GPO, je otevřít politiku v novém operačním systému. Kliknout pravým tlačítkem na Administrative Templates a zvolit Add/Remove Templates a odstranit všechny připojené soubory. [5]

Záloha politik - lze provést kliknutím pravým tlačítkem myši na Group Policy Objects v Group Policy Management Console a volbou Back Up All. [5]

Konverze ADM souboru do ADMX - Pro převod starých ADM šablon na nové ADMX lze využít nástroj ADMX Migrator. Ten lze také využít k editaci ADMX souboru nebo k vytvoření nového. [5]

3.9.1 Vyhledávání a filtrování v Administrative Templates

V minulosti byl vždy docela velký problém cokoliv v nastavení politik rychle nalézt. Je to dáno tím, že položek je zde několik tisíc a chyběla jakákoliv základní možnost rychlého a efektivního vyhledávání. Dnes jsou již naštěstí k dispozici dvě důležité pomocné operace, zobrazení všech položek na jednom místě a filtrování. [5]

Nově je v administračních nástrojích pro editaci GPO (GPOE, GPME), pod položkou Administrative Templates, k dispozici ještě složka All Settings, která obsahuje kompletně všechna nastavení ze všech načtených ADM/ADMX souborů. Takže je snadné vyhledávat položky podle jména. [5]

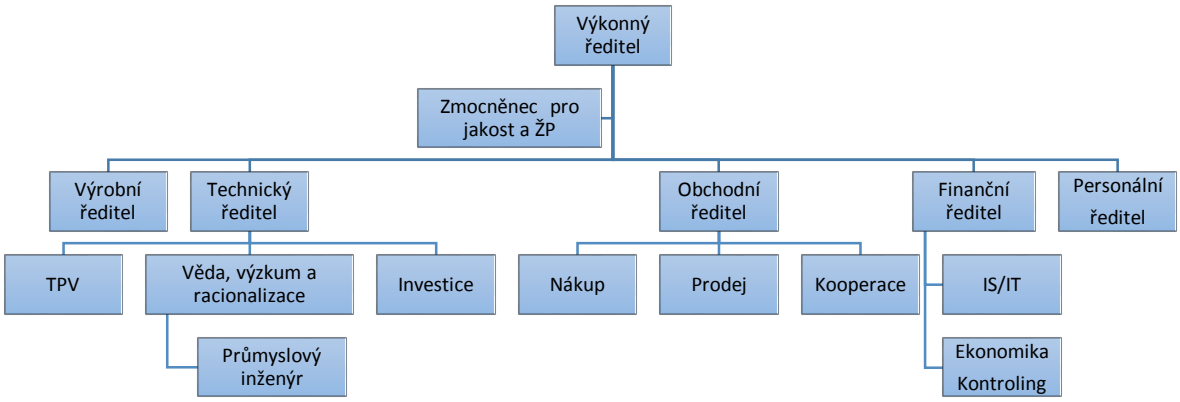
Druhou novinkou editovacích nástrojů je možnost přehledného filtrování nastavení z ADMX souborů. Když kliknutím pravého tlačítka na Administrative Templates nebo nějakou podsložku, se objeví v kontextovém menu položky Filter On a Filter Options.

Když je vybrán Filter Options, tak se zobrazí dialog, kde je možno zadat parametry filtrování. Lze si vypsat položky, které jsou nastavené (Configured), u kterých je komentář (Commented), které jsou určeny pro určitou platformu (Requirements Filters). A asi hlavní a nejdůležitější je filtrování podle klíčových slov (Keyword Filters), kde zadáním jednoho nebo více slov se dá určit jeho výskyt v názvu politiky, popisu či komentáři. Po kliknutí na OK se rovnou filtrování zapne (Filter On). [5]

II. PRAKTICKÁ ČÁST

4 ORGANIZAČNÍ STRUKTURA SPOLEČNOSTI V NÁVAZNOSTI NA ACTIVE DIRECTORY

Organizační struktura Active Directory ve firmě Kovárna VIVA a.s. vychází z organizační struktury společnosti uvedené na tomto obrázku:

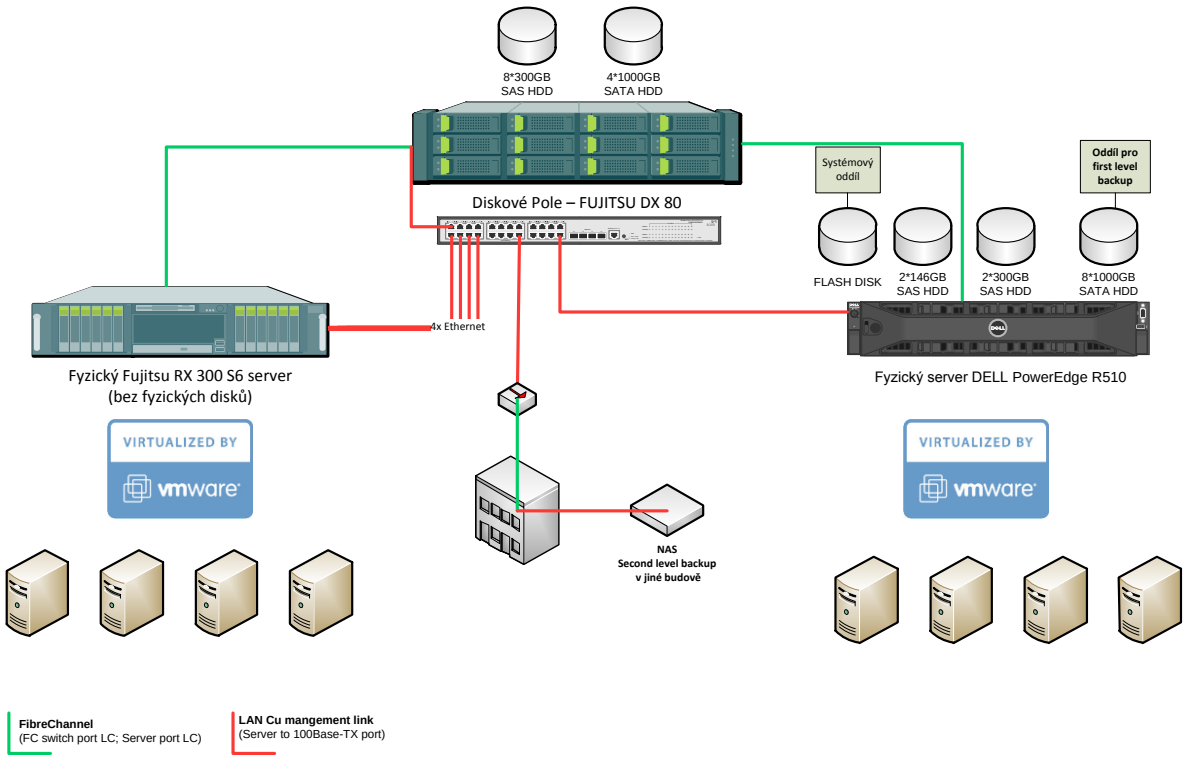


Obr. 12. Organizační struktura společnosti

Dále jsou organizační jednotky děleny na samostatně hospodařící střediska.

4.1 Představení vnitřní sítě Kovárny VIVA a.s.

Uspořádání síťové IT infrastruktury.



Obr. 13. – Serverová IT infrastruktura (interní materiály)

Životnost hardware i software serverů bylo oddělením IS/IT a firmou stanoveno na 5 let. Proto v roce 2015 bude uskutečněna výměna zastaralého software a hardware.

4.2 Virtualizační Server Fujitsu RX300 S6

Na daný fyzický stoj byly umístěny virtuální stroje. Virtuálním prostředím je VMware vSphere. Následující rozpis přesně specifikuje virtuální servery běžící na daném fyzickém stroji, včetně rozmístění aplikací, služeb a software provozovaných společností Kovárna VIVA a.s :

- server s operačním systémem Linux Debian 5.0 na kterém je nainstalován Informační systém ABAS

- aplikační server postavený na operačním systému Windows server 2003 32 bit, kde jsou nainstalovány tyto aplikace:
    - Aktion – docházkový a vykazovací systém
    - PERM – personalistika amzdy
    - CP server – plánování výroby
    - Symantec Endpoint Protection server - centrální konzole antiviru
    - SafeQ – print server
- terminal server s OS Microsoft Windows Server 2008 R2 64bit, který poskytuje terminálové služby pro vzdálené připojení
- SQL server 2005 s OS Microsoft Windows Server 2008 64bit a aplikací TEAMCENTER (procesní software)
- zálohovací server postavený na OS Windows Server 2008 64bit a nainstalovaným zálohovací software AcronisESXAppliance

4.3 Virtualizační Server DELL PowerEdge510

Na daný fyzický stoj byly umístěny virtuální stroje. Virtuálním prostředím je VMware vSphere. Následující rozpis přesně specifikuje virtuální servery běžící na daném fyzickém stroji, včetně rozmístění aplikací, služeb a software provozovaných společností Kovárna VIVA a.s :

- management server s OS Windows Server 2008 R2 64bit jako primární řadič domény, DNS server, DHCP server a fileserver
- backup server jako mirror zálohovacího serveru postavený na OS Windows Server 2008 64bit a nainstalovaným zálohovací software AcronisESXAppliance
- Messaging Server s nainstalovaným Exchange serverem běžící na OS Windows Server 2008 R2 64bit a je také sekundárním řadičem domény.
- Security Server se softwarovým firewallem běžím na běžící na OS Windows Server 2008 R2 64bit

4.4 Souhrn fyzických a virtuálních serverů

Součásti infrastruktury je i další fyzický server s OS Windows Server 2008 R2 64bit, který je používán pro simulace tváření materiálu. Je to software FORGE francouzské firmy TRANSVALOR.

Takto je dán přehledný souhrn fyzických zařízení v sítí:

Tab. 1. Souhrn fyzických zařízení - servery a uložiště

ESXi2.viva.local (Dell)
IRMC management RX300 S6
ESXi1.viva.local (Fujitsu)
Eternus DX80 Diskové pole
Synology RS411 NAS

Virtuální stroje jsou umístěny na uložišti následovně:

Tab. 2. Tabulka virtuálních strojů

VM	Path
ABAS	[Diskove Pole - SAS RAID 6] ABAS/ABAS.vmx
AcronisESXAppliance(5)	[Diskove Pole - SATA 1] AcronisESXAppliance(5)/AcronisESXAppliance(5).vmx
AcronisESXAppliance(6)	[Diskove Pole - SATA 2] AcronisESXAppliance(6)/AcronisESXAppliance(6).vmx
BACKUPSERVER	[Diskove Pole - SAS RAID 6] BSERVER/BSERVER.vmx
LC-2000	[Diskove Pole - SATA 1] LC-2000/LC-2000.vmx
MAILSERVER	[Diskove Pole - SAS RAID 6] MAILSERVER/MAILSERVER.vmx
MONITORING	[Diskove Pole - SATA 1] monitoring/monitoring.vmx
SERVER2	[Diskove Pole - SATA 2] SERVER2/SERVER2.vmx
SERVER4	[Diskove Pole - SAS RAID 6] SERVER4_1/SERVER4_1.vmx
TCE	[Diskove Pole - SATA 3] TCE1/TCE1.vmx
TERMINALSERVER	[Diskove Pole - SAS RAID 6] TERMINAL/TERMINAL.vmx
TMG	[Diskove Pole - SAS RAID 6] TMG/TMG.vmx
VM	Path

5 ANALÝZA ACTIVE DIRECTORY - STÁVAJÍCÍ STAV

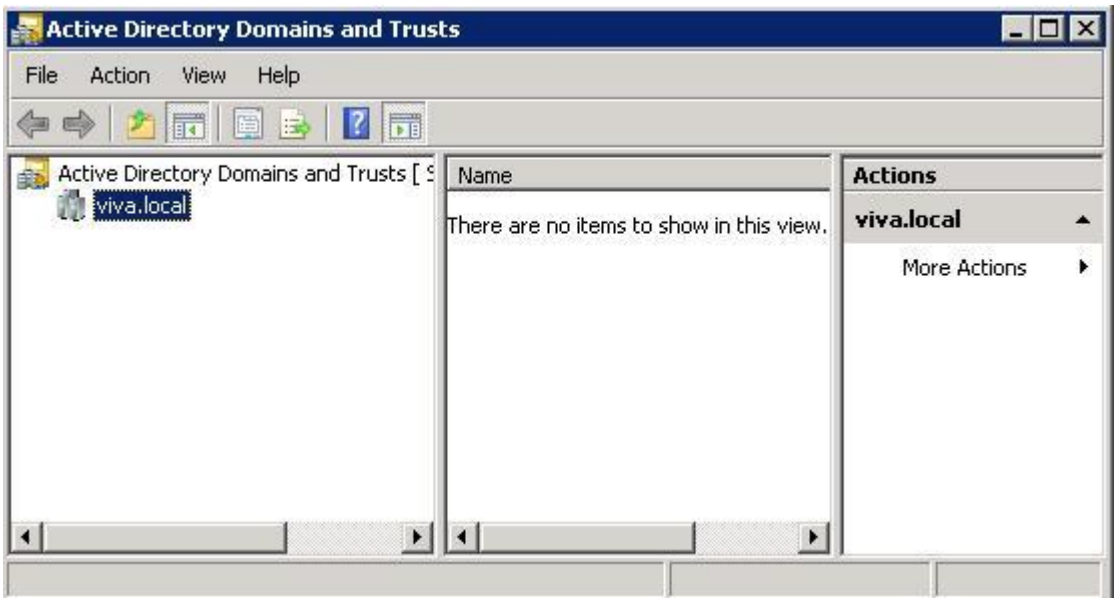
Úroveň funkčnosti domény a doménové struktury Active Directory je v režimu 2008.

5.1 Nástroje pro správu služby Active Directory

Základními nástroji pro správu služeb Active Directory jsou:

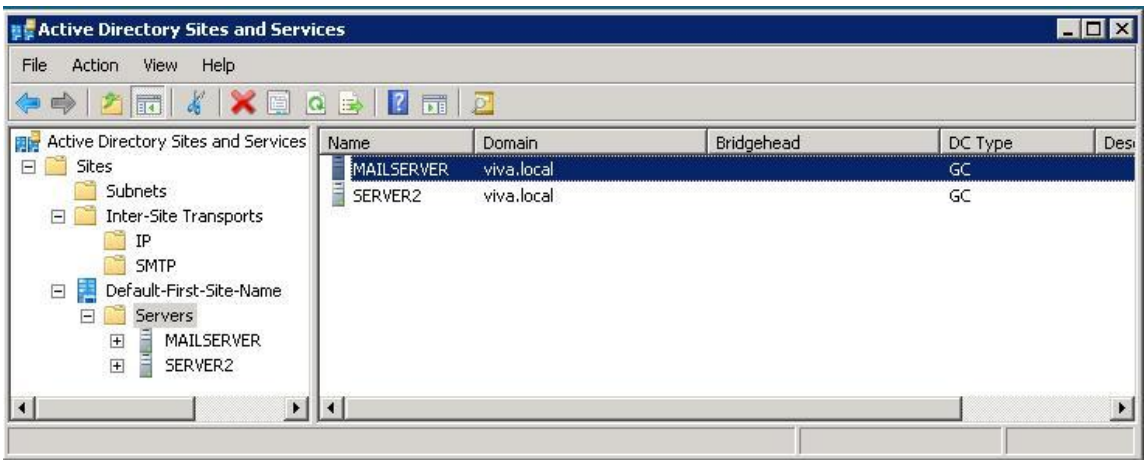
Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts), který je využíván ke spravování domén, doménových stromů a doménových struktur.

Ve firmě je použita a nastavena pouze jedna doména – viva.local. Tím je všechno nastavení v AD prováděno jednoduše a přehledně.



Obr. 14. Domény a vztahy důvěryhodnosti služby Active Directory

Lokality a Služby Active Directory (Active Directory Sites And Services). Tento grafický nástroj se používán ke správě a údržbě lokalit a podsítí.

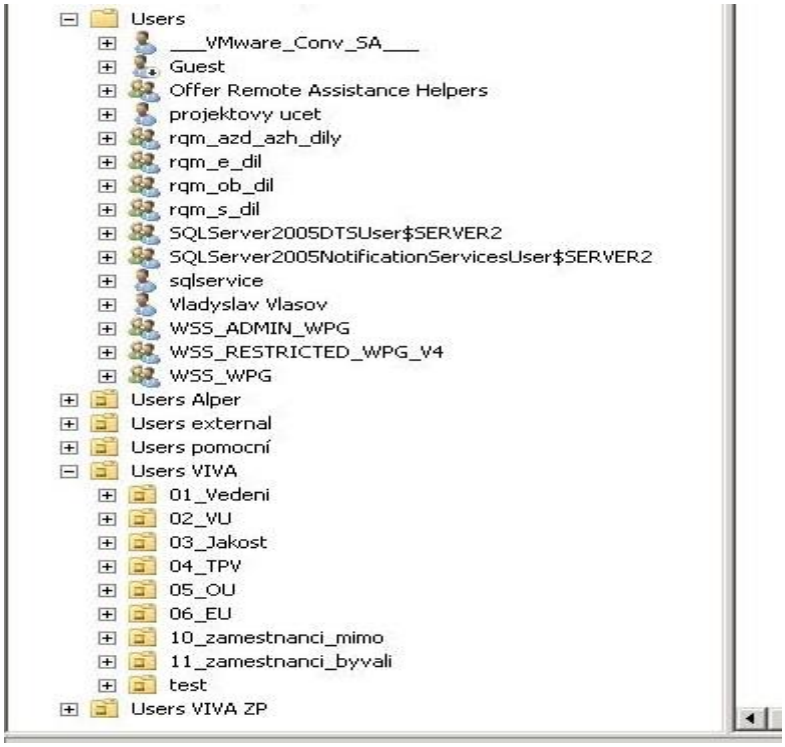


Obr. 15. Active Directory Sites And Services

Podsítě nejsou nastaveny. V Default-First- Site-Name v podsložce Servers jsou nastaveny dva DNS Servery. Server2 jako hlavní DNS server a MAILSERVER jako záložní.

Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).

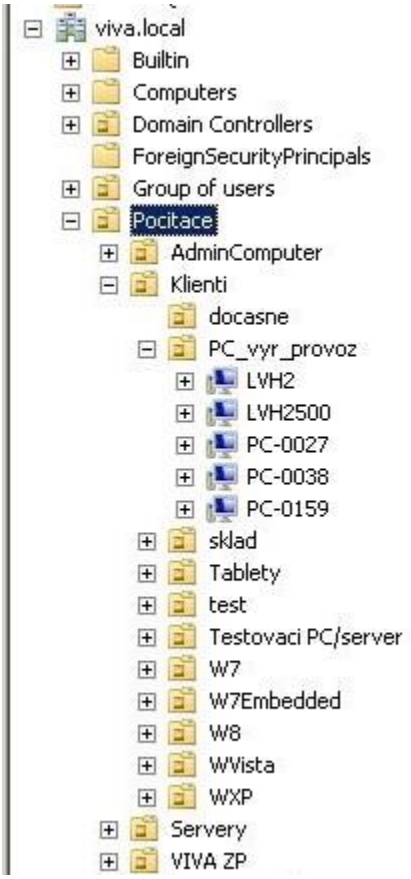
Zde bude první věnována pozornost nastavení pro počítače a uživatele. Bude to velmi důležité, protože bude dále využíváno pro nastavení zásad skupin GPO.



Obr. 16. Uživatelé služby Active Directory

Uživatelé jsou zavedeni do organizačních jednotek podle útvarů firmy a potom jsou dále tyto útvary rozděleny do středisek firmy. Dále jsou zde uvedeny organizační jednotky uživatelů:

- Alper – pobočná firma (Prostějov)
- Externí – uživatelé s firem zabývající se opravami strojů, software, atd
- Pomocní – uživatelé vytvořeni účelově pro potřeby správy
- VivaZP - středisko pro obrábění (součást areálu Kovárny VIVA a.s.)



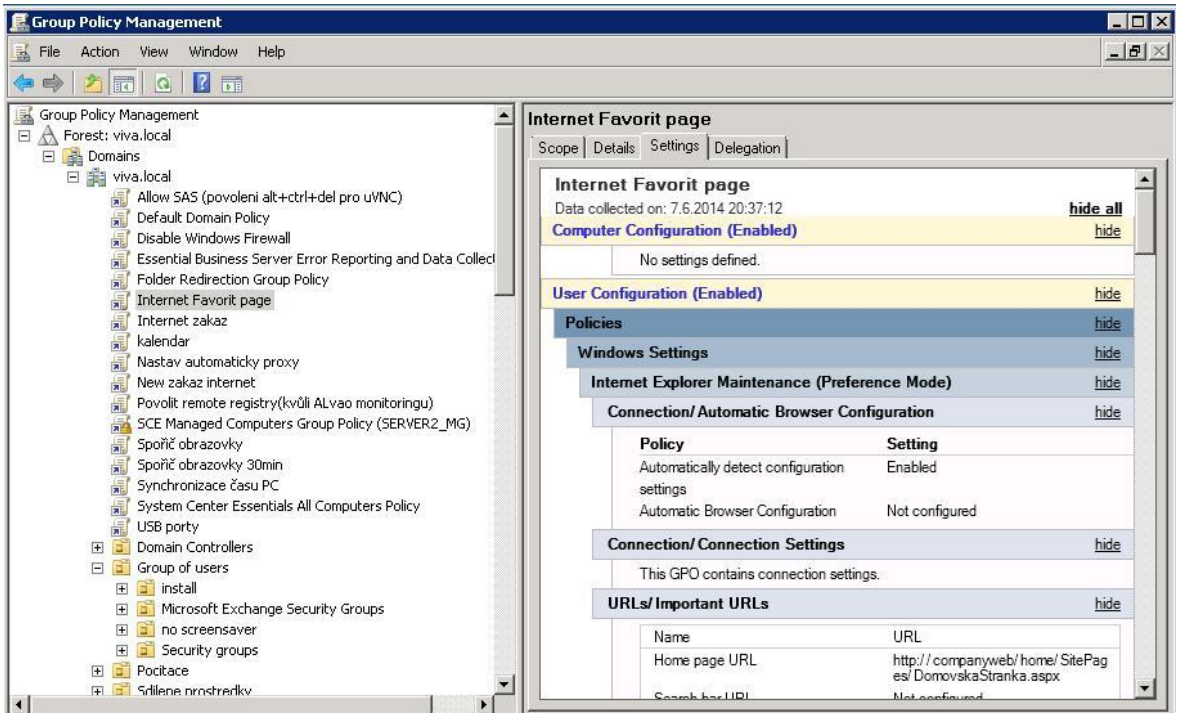
Obr. 17. Počítače služby Active Directory

Počítače jsou rozděleny organizačních jednotek podle operačních systémů. Tato organizační jednotka je dále rozdělena na 32bit a 64bit například u Windows 7, Windows Vista, Windows XP a Servery. Do organizační jednotky dočasné jsou dávány počítače pro účely dočasného testování software, atd. V organizační jednotce PC_vyr_provoz jsou počítače pro komunikaci s výrobními stroji (hlavně při poruchách), kde ještě nebyla provedena výměna za spolehlivé systémy Embeded.

Editor ADSI (ADSI Edit). Běžně je používán k editaci ADSI (Active Directory Service Interfaces). Aby byl efektivně využíván, je zapotřebí i znalosti prostředí PowerShell.

6 ANALÝZA ZÁSAD SKUPIN GPO (GROUP POLICY OBJECT) VE WINDOWS

Na virtuálním stroji Server2 je nainstalován grafický nástroj pro správu a pro práci se službou Zásady skupin GPO v podobě modulu ***Group Policy Management Console***.

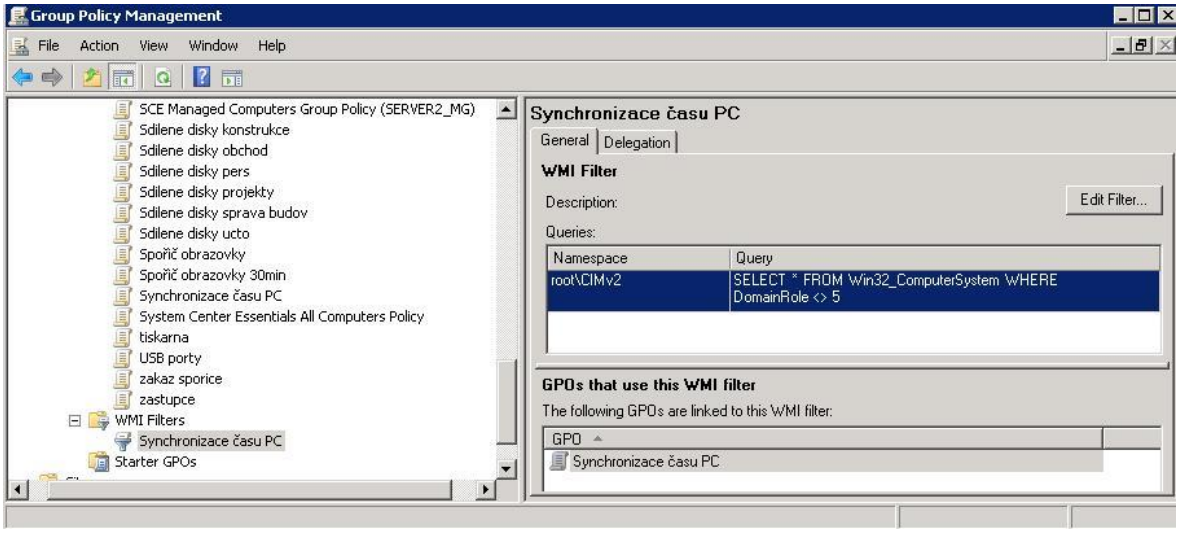


Obr. 18. Group Policy Management Console

Jsou zde nastaveny restrikce, účelová nastavení, pomocná nastavení, instalace software, a další nastavení jako jsou:

- Tvorba, úprava nebo mazání objektů zásad skupiny (GPO).
- Kopírování, import a export všech objektů (GPO).
- Zálohování tak i obnova objektů GPO.
- Modelování objektů GPO před ostrým nasazením, takže je možné dopředu zjistit, jak bude tímto nastavením ovlivněn uživatel nebo počítač.
- Modelování již aplikovaných objektů GPO, aby bylo zjištěno, jak ovlivní počítač nebo uživatele.

6.1 Filtry Rozhraní WMI(Windows Management Instrumentation)



Obr. 19. Příklad použití filtru WMI pro synchronizaci času PC

Technologie WMI, to je řídící struktura, přes kterou je dotazováno na základní atributy počítače. Je tedy používána k dotazu, jaký vlastně je na počítači operační systém nebo jak velké množství operační paměti má tento počítač dostupné.

Skutečně velmi významnou se stává tato technologie, pokud je používáno více filtrů rozhraní WMI. Více dotazů WMI složí k tomu, aby byly ověřovány určité podmínky.
Potom když je spojen filtr WMI s objektem GPO, dochází k tomu, že jsou řízeny aplikace zásad, protože systémem zásad jsou vyhodnoceny dotazy WMI v kontextu počítače, na kterém jsou zásady uplatňovány. Jestli je vrácena hodnota pravda, potom je splněno požadované kritérium a nastavení GPO se uplatní.

6.2 Návrh na lepší využití a nastavení Active Directory

V podstatě není nikde dána, ani neexistuje universální šablona nastavení Active Directory pro uspořádání Organizačních jednotek v ní. Z vlastní praxe je to vnímáno tak, že toto uspřádání se postupně mění s vývojem firmy.
Pokud někde je předkládána ideální šablona pro nastavení AD, tak je to spíše dáno subjektivním názorem předkladatele.

Na základě analýzy stávajícího stavu a potřeb firmy byly navrhnuty následující úpravy:

1. Bude vytvořen (ve spolupráci s personálním oddělením) firemní katalog pracovních zařazení. Tento katalog bude zanesen do Active Directory např.:
   - Nákupce
   - Skladník
   - Mistr výroby
   - Kontrolor
   - Expedient
   - Účetní

Ke každému pracovnímu zařazení budou přiřazeny práva Secure Group a zařazení do Distribution Group.
Bude vytvořen list pracovního zařazení s kompletním výpisem všech práv a distribučních skupin této pracovní pozice.
Tento list bude potom odsouhlasen nadřízeným této konkrétní pracovní pozice.
Potom bude velmi zjednodušen systém zavedení nového pracovníka na určitou pracovní pozici, bez rizika udělení nevhodných vyšších práv, které nepřísluší určité pracovní pozici.

2. Pro další využití, které bude používáno pro nastavení zásad GPO, budou vytvořeny organizační jednotky jako bezpečnostní zóny, např.:
   - Bezpečnostní zóna č.1
   - Bezpečnostní zóna č.2
   - Bezpečnostní zóna č.3

   Do těchto zón budou přiřazeny určité počítače, nebo další zařízení. Popis nastavení zón pro zásady skupin GPO bude proveden v návrhu nastavení zásad skupin GPO.

3. Budou nastaveny organizační jednotky pro vzdálenou instalaci přes zásady skupin GPO např.:

   - Teamcenter
   - Unigraphics
   - Aktion
   - Lookeen
   - Alvao
   - ProgeCad
   - Internet Explorer
   - Forge

   Význam bude popsán v návrhu a využití zásad skupin GPO.

7 NÁVRH, VYUŽITÍ A NASTAVENÍ ZÁSAD SKUPIN GPO

Některé nastavení zásad skupin byly zkoušeny na firmou zapůjčené Workstation s těmito parametry:

Workstation LENOVO S30:
- Procesor Intel Xeon CPU E5-1620/3,6GHz
- Operační paměť RAM 8GB
- HDD 2 TB
- Operační systém Microsoft Windows 7 Pro - 64bit

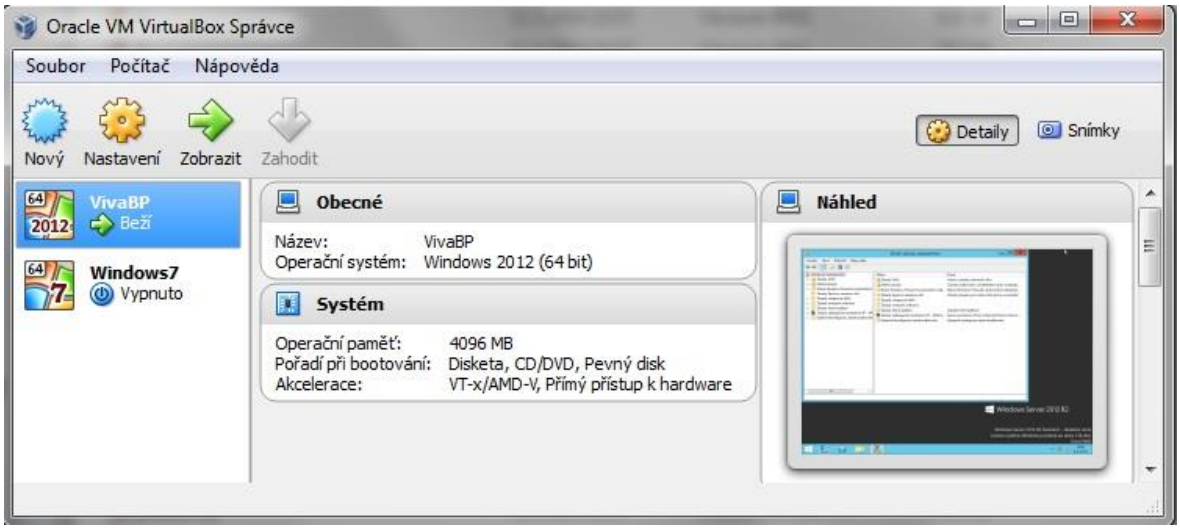
Dále bylo využito:

- Software pro virtualizaci – Oracle VM VirtualBox.
-

V něm byly nainstalovány :

- Windows Server 2012 R2/64bit – jako server
- Windows 7 / 64bit – jako uživatelská stanice

Windows Server 2012 R2 byl nainstalován a testován z důvodu přechodu firmy v roce 2015 na tento nový software.

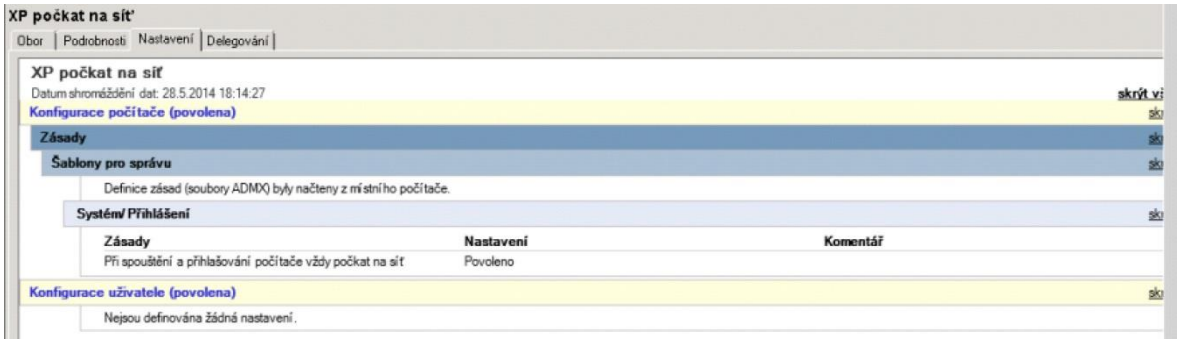


Obr. 20. Oracle VM VirtualBox s testovacím Software

7.1 Testované nastavení zásad skupin GPO

7.1.1 Čekání na síť pro Microsoft Windows XP

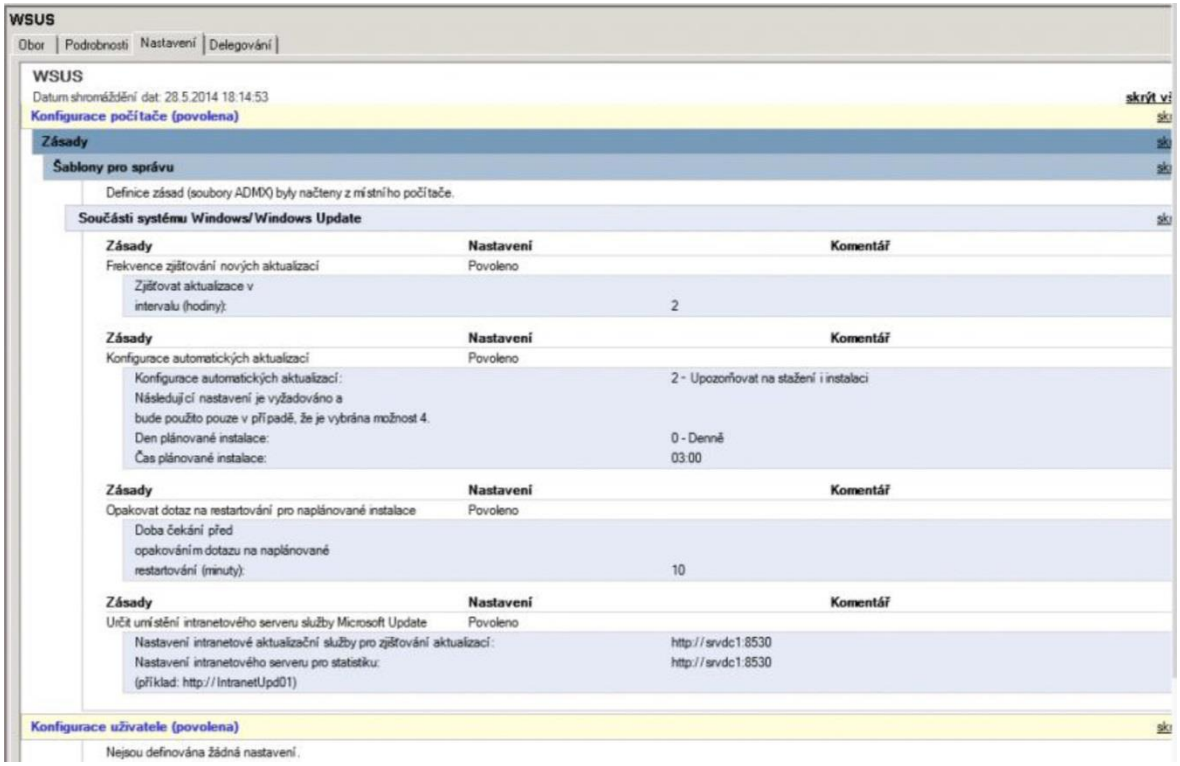
Aby byly vždy aplikovány všechny politiky ze zásad skupin GPO, je nutné, aby bylo nastaveno v zásadách politik GPO, čekání na síť. Tím bude odstraněno to, že nastavení některé politiky nebylo provedeno. Pokud toto není nastaveno, jsou provedeny jen politiky stávající a nová politika ne.



Obr. 21. Nastavení Windows XP čekání na síť

7.1.2 Windows Server Update Service (WSUS)

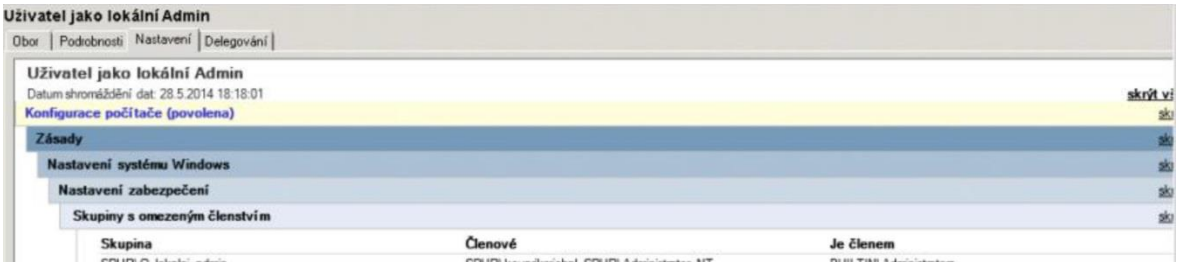
Určitě by měla být využívána v novém systému Windows Server 2012 služba WSUS, která je integrována do operačního systému jako jedna role serveru.
Bude tím umožněno spravovat distribuce všech aktualizací vydaných prostřednictvím služby Microsoft Update a to do všech počítačů ve firemní síti.



Obr. 22. Nastavení WSUS serveru

7.1.3 Nastavení - uživatel jako lokální Admin

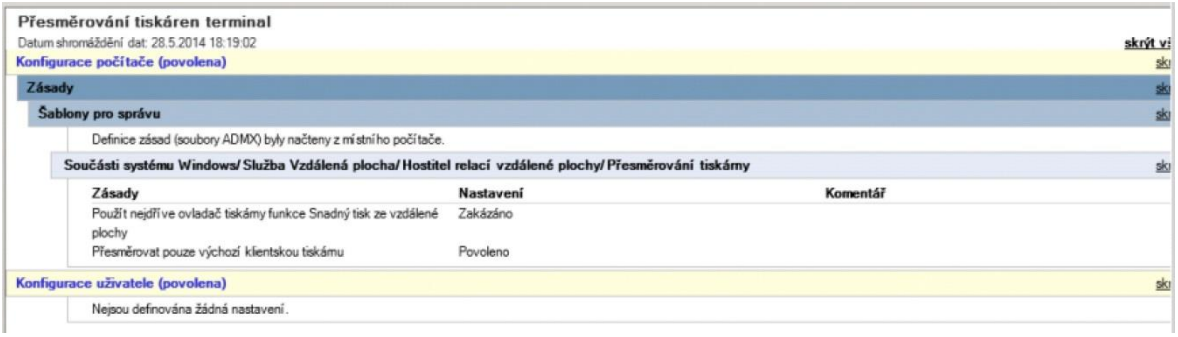
Velmi frekventované nastavení zásad skupin GPO, kterým je umožněno, komfortní a rychlá změna u uživatele, pro různé účely instalace software na počítač.



Obr. 23. Nastavení uživatele jako lokální Administrátor

7.1.4 Nastavení přesměrování tiskáren na terminál

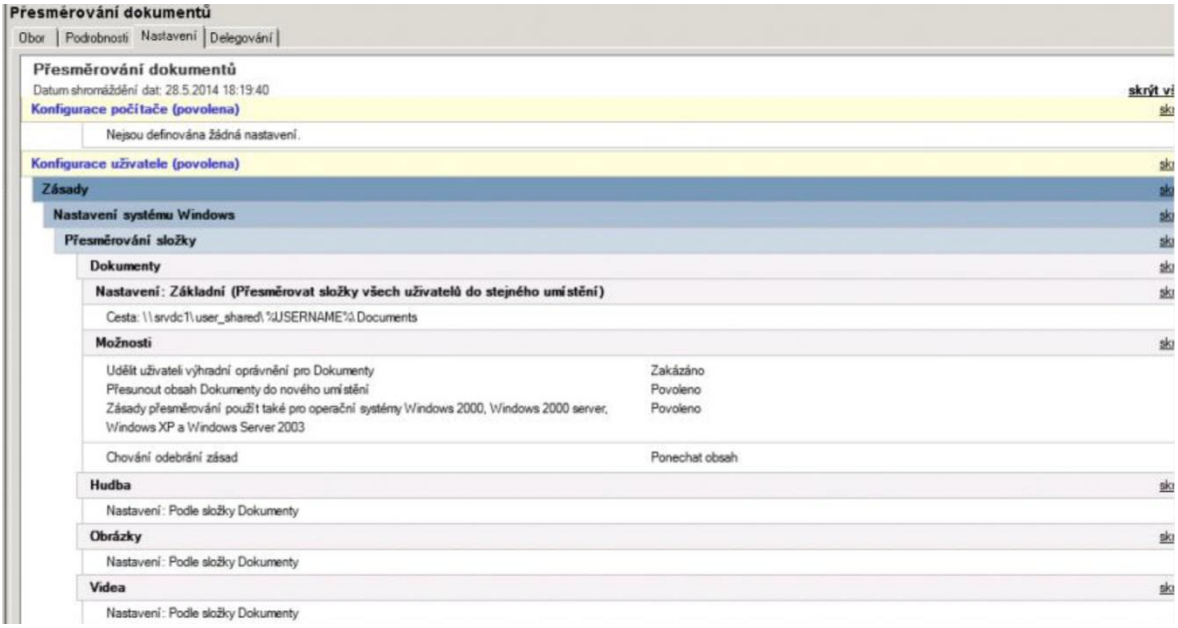
Velmi praktická zásada skupin GPO pro použití přesměrování tiskárny na Terminal.



Obr. 24. Nastavení přesměrování tiskárny na terminál pomocí zásad skupiny GPO

7.1.5 Nastavení přesměrování dokumentů

Další jedno z frekventovaných nastavení, které je velmi často používáno ve firmách, aby se předcházelo ztrátám dat na lokálním disku počítače.



Obr. 25. Nastavení přesměrování dokumentů pomocí zásad skupiny GPO

7.2 Využití nastavení zásad skupiny GPO z návrhu Active Directory

1. Pomocí zásad skupin budou nastaveny tyto bezpečnostní zóny:
    1. Bezpečnostní zóna jako zóna s nejvyššími restrikcemi
        - Zákaz Internetu
        - Zákaz instalace software
        - Zákaz instalace hardware
        - Zákaz úpravy plochy
        - Zákaz tisku

    2. Bezpečnostní zóna se středním zabezpečením.
        - Zákaz instalace software
        - Zákaz instalace hardware
        - Zákaz úpravy plochy
        - Tisk povolen
        - Internet povolen

    3. Bezpečnostní zóna s nejnižším zabezpečením
        - Zákaz instalace software
        - Zákaz instalace hardware
        - Povolena úprava plochy
        - Tisk povolen
        - Internet povolen

Samozřejmě, že všeho musí být používáno s mírou a není možné, aby byla prodlužována doba přihlášení uživatele, protože je zpracováváno mnoho zásad skupiny GPO.

2. Pomocí zásad skupin GPO aby byl instalován Software jiných stran (myšleno ostatní Software mimo Microsoft).
   V Active Directory budou již vytvořeny organizační jednotky typu:

   - Teamcenter
   - Unigraphics
   - Aktion
   - Lookeen
   - Alvao
   - ProgeCad
   - Internet Explorer
   - Forge

Ty budou použity pro uživatele, kteří potřebují nainstalovat jednotlivý Software na svůj počítač. Protože, pokud jsou instalovány některé software lokálně na počítač (nelze vytvořit MSI (Microsoft Installer Package) balíček je to velká časová ztráta pro administrátora. Díky novým verzím Software Unigraphics a Teamcenter by měl být tento problém již odstraněn.

8. Zhodnocení úspory navrhnutých řešení

Celý návrh Active Directory a zásady skupiny GPO by byl řešen jako interní projekt firmy s propočítanými náklady a přínosy pro firmu Kovárna VIVA a.s.

Celkový projekt bude vypracován i s časovým plánem realizace a kompletním popisem jednotlivých fází projektu. Rychlé hodnocení přínosů by bylo zkresleno subjektivním hodnocením zpracovatele.

V podmínkách testování je nemožné, aby bylo plně simulováno pracovní prostředí celé firmy a proto finanční zhodnocení přínosů nebude úplně přesné.

Jednoznačně bude už finančním přínosem pro firmu přechod na platformu Microsoft Server 2012 R2 A Microsoft SQL Server 2012. Také efektivnější využití nastavení Active Directory a zásad skupin GPO již na Microsoft Serveru 2012 R2 přispěje k zjednodušení práce v oblasti administrace a tím i k finančním úsporám firmy.

Výpočet úspory navrhnutého řešení byl realizován podle vzorce:

Přínosy – Náklady = Úspory

Náklady:

- Windows Server 2012 R2 + 150 licencí ……115 950,-Kč bez DPH

Účetně se Software odpisuje 3 roky.

- Windows Server 2012 R2 / 1 rok …… 38 650,-Kč bez DPH

Náklady na 1 hodinu Správce sítě …… 500,-Kč bez DPH

Časová náročnost instalace Software (na PC) Unigraphics ……..0.5 hod
Časová náročnost instalace Software (na PC) Teamcenter ……...0.5 hod
Software Unigraphics 4x/rok upgrade
Software Teamcenter 3x/rok upgrade
Počet instalací Unigraphics…….18
Počet instalací Teamcentru …….40
Unigraphics – časová náročnost lokálních instalací za rok…… 9x4=36 hod
Teamcenter – časová náročnost lokálních instalací za rok ……20x3=60 hod
Celkem časová náročnost instalací Teamcentru a Unigraphics za rok……..96 hod
Celkové náklady na správce sítě při těchto instalací……..48 000,-Kč
Tyto náklady se stanou přínosem, pokud se využije vzdálené instalace.
Není počítán čas na přípravu, pro vzdálené instalace přes GPO, protože časová náročnost Lokální instalace je poněkud náročnější a tím je čas instalace poddimenzován.

Přínosy – Náklady = Úspora

48000 – 38650 = 9350

Potom roční úspora činí: **9 350,-Kč bez DPH**

ZÁVĚR

Díky nasazení nového software pro servery společnosti Kovárna VIVA a.s. a to Microsoft Server 2012 R2 a Microsoft SQL Server 2012. Bude velkým přínosem, vytvořit ve společnosti interní projekt na efektivní využívání služby Active Directory i Zásad skupiny Windows (GPO).

Na stávajícím Microsoft Serveru 2008 R2 jsou již některé nastavení problematické, jako například nastavení Internetových prohlížečů pomocí GPO , proto by bylo vhodné využít potenciálu nových technologií a plně se zaměřit na využití Zásad skupiny (GPO) ve Windows, které čítá několik tisíc možností nastavení.

Důležité je ovšem nepoužívat jakékoliv nastavení, ale jenom ty, které budou pro zvýšení efektivity práce administrátora. Není taky možné zahltit uživatele velkým množství politik GPO, které by pak měly kontraproduktivní účinek, a docházelo by k velkému čekání uživatelů na přihlášení z důvodů zpracovávání nepřeberného množství politik.

SEZNAM POUŽITÉ LITERATURY

[1] Co je nového v zásadách skupiny. MICROSOFT. Microsoft TechNet: Materiály pro IT odborníky [online]. © 2014 Microsoft [cit. 2014-06-11]. Dostupné z: http://technet.microsoft.com/cs-cz/library/2e7bfa32-9fa9-4031-8160-d3a8c526df8d#BKMK_gpupdate

[2] Týden s Windows Server 2012 R2: přístup uživatelů a ochrana informací. BILÍČEK, Michal. TechNet Blogs [online]. 6 Aug 2013 [cit. 2014-06-12]. Dostupné z: http://blogs.technet.com/b/technetczsk/archive/2013/08/07/tyden-s-windows-server-2012-r2-pristup-uzivatelu-a-ochrana-informaci.aspx

[3] STANEK, William R. Active Directory: kapesní rádce administrátora. Vyd. 1. Brno: Computer Press, 2009, 352 s. Kapesní rádce administrátora (Computer Press). ISBN 978-80-251-2555-7.

[4] Adresářové služby a LDAP. BOUŠKA, Petr. SAMURAJ: počítačové sítě, Cisco, Microsoft, VMware, administrace [online]. 14.09.2007 [cit. 2014-06-12]. Dostupné z: http://www.samuraj-cz.com/clanek/adresarove-sluzby-a-ldap/

[5] STANEK, William R. Group Policy: zásady skupiny ve Windows : kapesní rádce administrátora. Vyd. 1. Brno: Computer Press, 2010, 351 s. ISBN 978-80-251-2920-3.

[6] Co jsou skupiny zásad (Group Policy). SOUKUP, Ondřej. IT-Bloguje: Blog plný rad a návodů ze světa IT [online]. Pátek, 18 Září 2009 [cit. 2014-06-11]. Dostupné z: http://www.it-bloguje.cz/windows-server/active-directory/70-co-jsou-skupiny-zasad-group-policy.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
AD_DS	Active Directory Domain Services
ADM	Administrative Template
ADMX	Administrative Template
AD RMS	Active Directory Rights Manamegent Services
CIMOM	Common Information Model Object Manager
CSE	Client Side Extension
DHCP	Danamic Host Configuration Protocol
DNS	Domain Name System
GPC	Group policy Configuration
GPME	Group Policy Management Editor
GPO	Group Policy Object
GPOE	Group Policy Management Console
GPT	Group Policy Templates
HDD	Hard Disk Drive
IP	Internet Protocol
LAN	Local Area Network
LGPO	Local Group Policy Object
MAPI	Messaging Application Programming Interface
MMC	Microsoft Management Console
OU	Organization Unit
PC	Personal Computer
RAM	Random Access Memory
RSoP	Result of Policy
SAM	Security Accounts Manager
SAN	Storage Area Network
SaaS	Software as a Service
SYSVOL	System Volume

WAN	Wide Area Network
WMI	Windows Management Instrumentation

SEZNAM OBRÁZKŮ

Obr. 1. Nové funkce v systému Windows Server 2012 R2 [1] 13
Obr. 2. Přidávání Server Roles v Microsoft Server 2012 R2 [2] 14
Obr. 3. Schéma - Automatic VPN Connections ve Windows Server 2012 R2 [2] 14
Obr. 4. Schéma pro Dynamic Access Control [2] 15
Obr. 5. Služba Active Directory a její spolupráce s jinými klienty [3] 17
Obr. 6. Běžné atributy používané v Active Directory [4] 19
Obr. 7. Část adresáře Active Directory [4] 19
Obr. 8. Jmenné atributy a ekvivalenty pro AD [4] 20
Obr. 9. Operace LDAPu [4] 20
Obr. 10. Možné nastavení na každé politice GPO [5] 25
Obr. 11. Možnost změny aplikace GPO při pomalé lince 29
Obr. 12. Organizační struktura společnosti 35
Obr. 13. – Serverová IT infrastruktura (interní materiály) 36
Obr. 14. Domény a vztahy důvěryhodnosti služby Active Directory 39
Obr. 15. Active Directory Sites And Services 39
Obr. 16. Uživatelé služby Active Directory 40
Obr. 17. Počítače služby Active Directory 41
Obr. 18. Group Policy Management Console 42
Obr. 19. Příklad použití filtru WMI pro synchronizaci času PC 43
Obr. 20. Oracle VM VirtualBox s testovacím Software 45
Obr. 21. Nastavení Windows XP čekání na síť 46
Obr. 22. Nastavení WSUS serveru 46
Obr. 23. Nastavení uživatele jako lokální Administrátor 47
Obr. 24. Nastavení přesměrování tiskárny na terminál pomocí zásad skupiny GPO 47
Obr. 25. Nastavení přesměrování dokumentů pomocí zásad skupiny GPO 48

SEZNAM TABULEK

Tab. 1. Souhrn fyzických zařízení - servery a uložiště 38
Tab. 2. Tabulka virtuálních strojů 38