Implementace Active Directory Domain Services

Implementation of Active Directory Domain Services

Bc. Ondřej Kořínek

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Ondřej KOŘÍNEK**
Osobní číslo:	**A08405**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Implementace Active Directory Domain Services**

Zásady pro vypracování:

1. **Zpracujte návrh implementace Windows Server 2008 R2 Active Directory Domain Services do prostředí UTB ve Zlíně.**
2. **Analyzujte stávající stav.**
3. **Navrhněte:**
   - **strukturu domény,**
   - **rozmístění řadičů domény a lokalit,**
   - **organizační jednotky nejvyšší úrovně UTB ve Zlíně,**
   - **podrobnou strukturu organizačních jednotek a skupin pro FAI,**
   - **jmenné konvence pro uživatele, počítače, lokality a servery,**
   - **infrastrukturu DNS,**
   - **scénáře správy zásad skupin pro FAI.**
4. **Otestujte ve virtuálním prostředí řadič domény pro FAI.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **REIMER, Stan, KEZEMA, Conan, MULCARE, Mike. Windows Server 2008 Active Directory : Resource Kit. Redmond, Washington : Microsoft Press, 2008. 827 s. ISBN 2008920569.**
2. **HOLME, Dan, RUEST, Nelson, RUEST, Danielle. Configuring Windows Server 2008 Active Directory : Training Kit. Redmond, Washington : Microsoft Press, 2008. 951 s. ISBN X14-15141.**
3. **MAR-ELIA, Darren, MELBER, Derek, STANEK, Wiliam S. Zásady skupin Microsoft Windows : Microsoft Windows Group Policy Guide. Brno : Computer Press a.s., 2006. 760 s. ISBN 80-251-1261-4.**
4. **RUSSEL, Charlie, CRAWFORD, Sharon. Microsoft Windows Server 2008 : Velký průvodce administrátora. Brno : Computer Press a.s., 2009. 1271 s. ISBN 978-80-251-2115-3.**
5. **STANEK, William R. Mistrovství v Microsoft Windows Server 2008. Brno : Computer Press a.s., 2009. 1368 s. ISBN 978-80-251-2158-0.**
6. **Microsoft Corporation. 6424A Fundamentals of Windows Server 2008 Active Directory : Microsoft Official Course. [s.l.] : [s.n.], 2008. 320 s. ISBN X14-69071.**

Vedoucí diplomové práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **8. června 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této diplomové práce je návrh implementace *Windows Server 2008 R2 Active Directory Domain Services* do prostředí Univerzity Tomáše Bati ve Zlíně.

Teoretická část objasňuje všeobecné poznatky o *Active Directory Domain Services*, dále pak charakterizuje základní role a služby operačního systému *Windows Server 2008 R2* důležité pro *AD DS*.

Praktická část, popisující současný stav UTB ve Zlíně, navazuje na design *Active Directory Domain Services*, vlastní konfiguraci a testy. Celou práci uzavírá kapitola o financování projektu.

Klíčová slova: Active Directory Domain Services, Doména, Lokalita, Doménový řadič, Subnet, Globální katalog, Zásady skupin, DNS, Windows Server

ABSTRACT

Target of this thesis is conception of a *Directory Domain Services* implementation into Tomas Bata University of Zlin environment.

The theory part is clearing up general knowledge on *Active Directory Domain Services* and further characterizes prime roles and services of *Windows Server 2008 R2* operation system important for *AD DS*.

The practical part is describing up-to-date status of UTB in Zlin, taking it up on *Active Directory Domain Services* design, true configuration as well as tests. The entire work is ended up with a chapter dealing with project financing.

Keywords: Active Directory Domain Services, Domain, Site, Domain Controller, Subnet, Global catalog, Group Policy, DNS, Windows Server

PODĚKOVÁNÍ

Rád bych poděkoval následujícím osobám:

Ing. Radko Řehákovi za výraznou podporu při studiu,

doc. Ing. Martinovi Syslovi, Ph.D., vedoucímu mé diplomové práce, za podnětné připomínky, jež mi umožnily úspěšné zpracování této práce.

A především mé ženě Mirce, dcerce Magdaléně a synkovi Robertovi za neobyčejnou trpělivost.

Věnováno mému otci.

MOTTO

„*Každá dostatečně pokročilá technologie je k nerozeznání od magie.*“

Arthur C. Clarke

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/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 diplomovou/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 – diplomovou/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 diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Počítače, propojené do sítě, jsou bez pochyby již velmi běžnou součástí našeho života. Položme si otázku: „Co je základem počítačové sítě?“ Ať budou odpovídat správci sítí nebo běžní uživatelé, jejich odpovědi budou postaveny na společné podstatě, kterou je sdílení informací.

Nabízí se další otázka: „Kdy je síťový operační systém morálně zastaralý?“ Existuje mnoho společností, které tuto otázku vůbec neřeší a pouze se zaměřují na funkčnost. Na druhou stranu morální zastaralost je strašákem dnešních dní a dá se s jistou dávkou ironie říci, že ve chvíli nákupu je jakákoliv IT morálně zastaralá.

Není třeba polemizovat nad faktem, že životní cyklus síťového operačního systému *Novel Netware 6.5* končí, protože byl ukončen vývoj a předpokládá se konec technické podpory. Tato skutečnost je známá i pověřeným pracovníkům na Univerzitě Tomáše Bati ve Zlíně, která tento systém používá, a proto bylo navrženo řešení implementovat *Windows Server 2008 R2*.

Motivací této diplomové práce je prohloubení již nabitých teoretických i praktických znalostí funkcionalit *Active Directory Domain Services* a cílem práce je aplikovat získané vědomosti na modelový návrh implementace *AD DS*, který by mohl nahradit stávající technologii.

V teoretické části je vysvětlena terminologie *Active Directory Domain Services*, jeho běžné funkce a jsou přiblíženy role systému, které jsou nezbytné pro základní implementaci.

Praktická část v úvodu analyzuje stav sítě Univerzity Tomáše Bati ve Zlíně. Dále předkládá návrh struktury *AD DS* s důrazem na efektivní zpřístupnění adresářových informačních zdrojů a služeb koncovým uživatelům prostřednictvím jednoho přihlášení. Řešení je v úzkém vztahu s bezpečnostními prvky koordinovanými z jednoho místa pro oblast rozsáhle sítě univerzity. Závěr kapitoly je věnován doporučeným školením a financování celého projektu.

I. TEORETICKÁ ČÁST

1 MICROSOFT WINDOWS SERVER 2008 R2

Systém *Windows Server 2008 R2* představuje dosud nejpokročilejší operační systém Windows Server, navržený pro podporu nové generace sítí, aplikací a webových služeb. Pomocí systému *Windows Server 2008 R2* je možné vyvíjet, distribuovat a spravovat komfortní uživatelská prostředí a aplikace, zajišťovat zabezpečenou síťovou infrastrukturu a zvyšovat technologickou vyspělost a hodnotu organizace. Systém *Windows Server 2008 R2* staví na pevných základech předchozích verzí platformy Windows Server, ale zároveň přináší cenné důležité funkce i významná vylepšení základního operačního systému. Nové webové nástroje, virtualizační technologie, vylepšení zabezpečení a nástroje pro správu přináší úsporu času, snižují náklady a vytváří pevný základ IT infrastruktury. [1]

1.1 Novinky Windows Server 2008 a distribuce R2

Každá nová verze systému s sebou nese předpoklad inovace již používaných funkcí a zároveň představení dalších progresivních funkcionalit, i když některé nemusejí být na první pohled patrné. Ty hlavní, které jsou obsažené v operačním systému *Windows Server 2008* a distribuce *R2* jsou:

- *Správce serveru (Server Management)* i rozšířená konzole *Microsoft Management Console*, umožňují konfigurovat a sledovat server z jednotného rozhraní a provádět běžné úkony administrace serveru s průvodci.
- Skriptovací jazyk a zároveň interpreter příkazového řádku *Windows PowerShell* poskytují automatizaci rutinních úkolů na mnoha serverech.
- *Zásady skupin (GPO)* rozšířené o skupinu *Předvoleb*, umožňují konfigurovat nastavení bez znalosti přihlašovacích skriptů.
- Optimalizovaná správa serveru a replikace dat vylepšují kontrolu nad servery v pobočkových sítích.
- Minimalistická instalace operačního systému s instalací pouze těch rolí a funkcí serveru, kterých je skutečně třeba.
- *Zálohování serveru (Windows Server Backup)* postavené na rychlejší technologii zálohování a zjednodušené obnově dat.
- *Windows Server 2008 Hyper-V* poskytuje virtualizaci serverových rolí i samotných virtuálních počítačů.

- *RemoteApps Terminálových služeb* a program *TS Web Access* umožňují otevřít vzdáleně aplikace tak, že vypadají jako by běžely na pracovní stanici koncového uživatele.
- *Network Access Protection* je jednou z rolí, která pomáhá chránit systémy i sítě proti počítačům s nevyhovujícím stavem v souladu s požadavky na zabezpečení.
- Program *BitLocker Drive Encription* přináší rozšířenou ochranu proti krádežím a vyzrazení dat v případě fyzické ztráty nebo krádeže serveru.[2, 3]

Tento seznam nových rolí a služeb není kompletní, protože se tato práce zaměřuje na *Active Directory Domain Services*, budeme o něco podrobněji novinkám v této roli.

1.1.1 Active Directory Domain Services

AD DS je neprávem opomíjená role valnou částí IT specialistů, i když jejich aplikace může mít zásadně pozitivní dopad na jejich síťové prostředí a systémy s ním spojené. Na druhou stranu je pravdou, že ne každá společnost je schopna ve své struktuře využít kompletní nabídku *AD DS*, ale každá prospěšná změna vedoucí k efektivnějšímu využití informačních technologií má smysl. Dále jsou uvedená některá zásadní vylepšení, která mohou pružně plnit tyto předpoklady:

- ***Read-Only Domain Controller*** – spravuje tytéž atributy a objekty služby *AD DS* jako řadič domény s možností zápisu, rozdíl spočívá v tom, že změny nelze provádět přímo, ale je použita replikace z *DC* do *RODC*.
- ***Restartovatelné AD DS služby*** – možnost zastavení služby a její následné spuštění.
- ***Fine Grained Password Policies*** – možnost definovat politiky pro hesla (komplexnost, délka hesla, apod.) a tyto politiky přiřazovat jednotlivým určeným *OU* či uživatelům.
- ***Audit změn*** – sledování a zaznamenávání změny objektů *AD DS*, tyto události obsahují původní i novou hodnotu parametru objektu.
- ***Zabránění nechtěnému smazání*** – nová automatická volba *Chránit proti nechtěnému smazání (Protect object from accidental deletion)*, která musí být deaktivována před smazáním objektu.
- ***Preferences*** – typické úkony – nastavení mapování disků, tiskáren, změna oprávnění na objektech, nastavení - např. VPN klienta, atd.
- ***Recycle Bin*** – po vymazání v *AD DS*, je možná obnova bez ztráty nastavení.

- ***Offline Domain Join*** – připojení operačního systému do domény *Windows Serveru 2008 R2* aniž je doména v době připojení dostupná.
- ***Best Practice Analyzer*** – v roli Správce serveru, lze vytvářet kontrolní seznam nad určenou rolí – využití při konfiguracích. [4, 5, 6]

1.2 Přehled edic operačního systému Windows Server 2008 R2

- ***Edice Windows Server 2008 R2 Foundation*** je určena pro malé organizace, kterým poskytne základ pro provozování nejčastěji používaných podnikových aplikací pro sdílení informací a prostředků.
- ***Windows Server 2008 R2 Standard*** je nejrobustnějším serverovým operačním systémem Windows v historii. Obsahuje integrované vylepšené technologie pro web a virtualizaci. Výkonné nástroje nabízejí větší kontrolu nad servery a optimalizují konfiguraci a správu. Rozšířené funkce pro zabezpečení posilují ochranu operačního systému, dat i sítě a zároveň vytvářejí pevnou, vysoce spolehlivou funkční základnu pro každou organizaci.
- ***Windows Server 2008 R2 Enterprise*** představuje pokročilou serverovou platformu, která poskytuje spolehlivější podporu nejdůležitějších úloh. Nabízí inovativní funkce pro virtualizaci, úsporu energie a snadnou správu a pomáhá usnadnit přístup mobilních pracovníků k firemním prostředkům.
- ***Windows Server 2008 R2 Datacenter*** představuje platformu pro nasazení nepostradatelných podnikových aplikací a rozsáhlou virtualizaci na malých i velkých serverech. Nabízí lepší dostupnost, vylepšené řízení spotřeby a integrovaná řešení pro pracovníky v terénu a pobočkách. Podporuje škálování od 2 do 64 procesorů.
- ***Windows Web Server 2008 R2*** představuje výkonnou platformu pro webové aplikace a služby. Tato edice obsahuje službu Internet Information Services (IIS) 7.5 a je navržena výhradně jako server připojený k Internetu.
- ***Edice Windows Server 2008 R2 pro systémy s procesorem Itanium*** podporuje škálování databází, podnikových a vlastních aplikací tak, aby splňovaly rostoucí potřeby podniku. Pomáhá zvýšit dostupnost díky clusteringu s podporou převzetí služeb při selhání a funkci dynamického dělení hardwaru. Virtualizuje nasazení

s možností spouštět neomezený počet virtuálních instancí systému Microsoft Windows Server. [8]

1.2.1 Hardwarové požadavky

Pro používání systému *Windows Server 2008 R2* je nutné následující vybavení:[1]

Tab. 1. Minimální hardwarové požadavky

Součást	Požadavek
Procesor	Minimum: 1.4 GHz (x64) Poznámka: Systém Windows Server 2008 R2 pro počítače s procesorem Itanium požaduje procesor Intel Itanium 2.
Paměť	Minimum: 512 MB RAM Maximum: 8 GB (Foundation) nebo 32 GB (Standard) nebo 2 TB (Enterprise, Datacenter a systémy s procesorem Itanium)
Volné místo na pevném disku	Minimum: 32 GB nebo více Foundation: 10 GB Poznámka: Počítače s více než 16 GB paměti RAM budou potřebovat více volného místa na pevném disku pro stránkování, hibernaci a odkládací soubory.
Zobrazení	Monitor s rozlišením Super VGA (800 × 600) nebo vyšším
Ostatní	Jednotka DVD-ROM, klávesnice a myš Microsoft Mouse nebo kompatibilní polohovací zařízení, připojení k síti Internet

[Zdroj: 7]

[1] Skutečné požadavky se budou lišit v závislosti na konfiguraci daného systému, aplikacích a funkcích, které jsou instalovány. Výkon procesoru závisí nejen na taktovací frekvenci procesoru, ale také na počtu jader a kapacitě mezipaměti procesoru. Požadavky na volné místo na disku pro systémový oddíl jsou pouze přibližné. Odhady požadovaného místa na disku pro operační systémy pro počítače s procesory Itanium a x64 se budou lišit. Další volné místo na disku může být požadováno v případě instalace přes síť. [7]

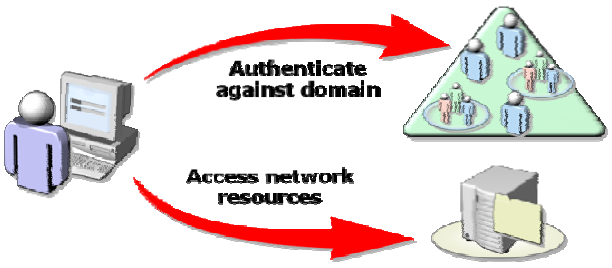
2 ACTIVE DIRECTORY DOMAIN SERVICES

Služba *AD DS* je srdcem domén založených na systému Windows už od dob svého představení v systému *Windows 2000*. Téměř každá úloha správy, kterou provedete, nějakým způsobem ovlivní *AD DS*. Služba *Active Directory Domain Service*s je založena na standardních internetových protokolech a je navržena tak, aby umožnila jednoznačně definovat strukturu sítě. [9]

AD DS zajišťuje ověřené vyhledávání a načítání informací tak, že odděluje do samostatných vrstev fyzickou a logickou strukturu adresářů. Fyzická vrstva určuje následující funkce:

- způsob přístupu k informacím v adresáři,
- způsob přístupu dat na pevném disku serveru.[10, 12]

Logická vrstva určuje, jakým způsobem jsou prezentovány informace obsažené v datovém úložišti a také řídí přístup k těmto informacím. Zajistí to definováním oborů názvů a názvových schémat, která jsou použita pro přístup k prostředkům uloženým v adresáři. A proto disponujeme takovou konzistentní metodou, kterou můžeme přistupovat k datům uloženým v adresáři bez ohledu na jejich typ.[12, 11]



Obr. 1. Uživatel versus AD DS [Zdroj: 14]

2.1 Infrastruktura služby

Nejvyšším prvkem v každé implementaci *AD DS* je kořenová doména struktury, která je založena při instalaci služby *Active Directory Domain Services* na prvním řadiči *(DC)* domény v nové doménové struktuře. Název kořenové domény, buď vlastní kořenové domény struktury, nebo kořenové domény nového stromu ve struktuře, funguje jako

základní název všech domén, které se v daném stromě vytvoří později. Domény ve stejné doménové struktuře mají následující vlastnosti:

- *Sdílené společné schéma* – všechny řadiče domény v doménové struktuře mají stejné schéma a doménovou strukturu – jediný hlavní server schémat.
- *Sdílejí společný oddíl adresáře konfigurace* – všechny řadiče domény mají společný kontejner konfigurace.
- *Sdílejí společnou konfiguraci vztahů důvěryhodnosti* – všechny domény v doménové struktuře jsou nastaveny tak, že důvěřují (obousměrně, tranzitivní) ostatním doménám ve struktuře.
- *Sdílejí společný globální katalog* – který ukládá částečnou repliku všech objektů v doménové struktuře.
- *Sdílejí společné správce pro celou doménovou strukturu* – všechny domény v doménové struktuře spravují na nejvyšší úrovni stejní správci – členové skupin Enterprise Admins a Schema Admins. [10, 11, 12]

2.1.1 Schéma

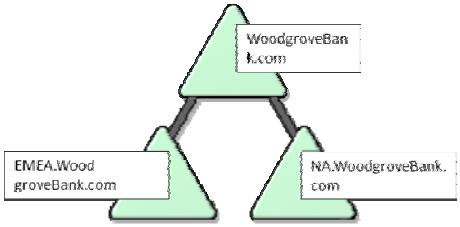
Obsahuje definici jednotlivých objektů, ze kterých se skládá adresář *AD DS*, např.: objekty, atributy, kontejnery. Výchozí schéma služby *AD DS* definuje nejběžnější třídy objektů, jako jsou uživatelé, skupiny, počítače, organizační jednotky, zásady zabezpečení a domény. [2, 14]

2.1.2 Doména

Doména *AD DS* je jednoduše skupina počítačů sdílejících společnou adresářovou databázi. Názvy domén *AD DS* musejí být jedinečné. Každá doména má své vlastní zásady zabezpečení a vytvořený vztah důvěryhodností s ostatními doménami. Domény mohou zahrnovat i více fyzických míst, takže se doména může skládat z více sítí a podsítí. V adresářové databázi domény jsou současně s objekty určující účty uživatelů, skupin, počítačů také sdílené prostředky, jako tiskárny nebo složky. [2]

2.1.2.1 Doménový strom

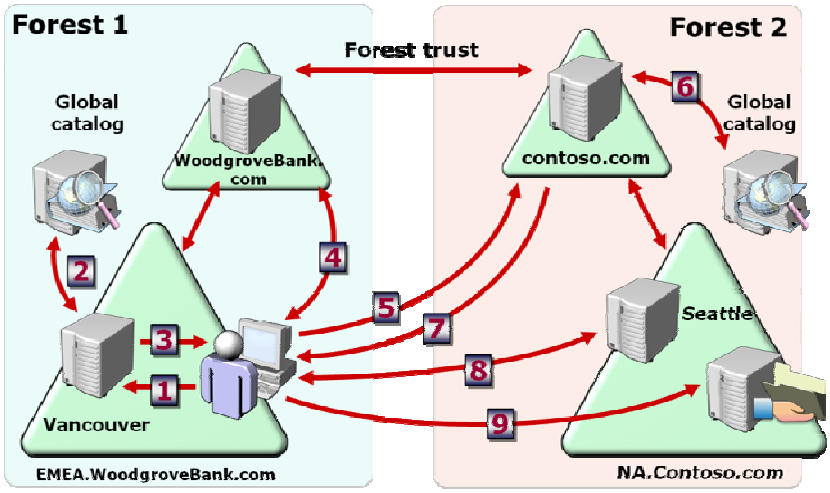
Souvislý obor názvů, ve kterém je každý název přímo odvozen z jediného názvu kořene. Díky tomu lze všechny listy nebo větve stromu nalézt procházením struktury od kořene podle jejich názvů. [16, 2]



Obr. 2. Doménový strom [14]

2.1.2.2 Doménový les

V zásadě je doménový les skupina doménových stromů, které sdílejí společný kořen oboru názvů. [2, 17]



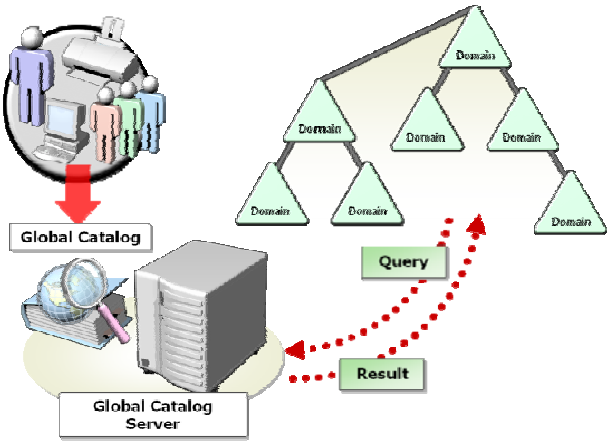
Obr. 3. Vztah důvěry - doménový les [14]

2.1.3 Globální katalog

Globální katalog (GC) je řadič domény, který ukládá kopie všech objektů služby *AD DS* v doménové struktuře. *Globální katalog* ukládá úplné kopie všech objektů v adresáři hostitelské domény a částečné kopie všech objektů v ostatních doménách v doménové struktuře. *Globální katalog* obsahuje částečné kopie všech objektů domény, které byly nejčastěji používány ve vyhledávacích operacích uživatelů. Tyto atributy jsou

v definici schématu označeny k zahrnutí do *Globálního katalogu*. Ukládání nejčastěji hledaných atributů všech objektů domény do *GC* umožňuje uživatelům efektivní vyhledávání, aniž by byl výkon sítě nepříznivě ovlivněn nepotřebnými odkazy na řadiče domény. *GC* tedy umožňuje nalézt informace z adresáře bez ohledu na to, v které doméně v lese se nachází. Jeho druhou funkcí je, že poskytuje informace o členství v *Univerzálních*

skupinách, které jsou potřeba při přihlašovacím procesu. Pokud není k dispozici *globální katalog* při přihlašování, uživatel se může přihlásit pouze lokálně na počítač. [21, 22]



Obr. 4. Globální katalog [Zdroj: 14]

2.1.3.1 Atribut

Atribut je jakákoliv dílčí informace, popisující nějaký aspekt zápisu. Sestává se z typu atributu a jedné nebo více hodnot atributu (příklad atributu: telefonní číslo a hodnota atributu: 456 678 890). [17, 2]

2.1.3.2 Objekt

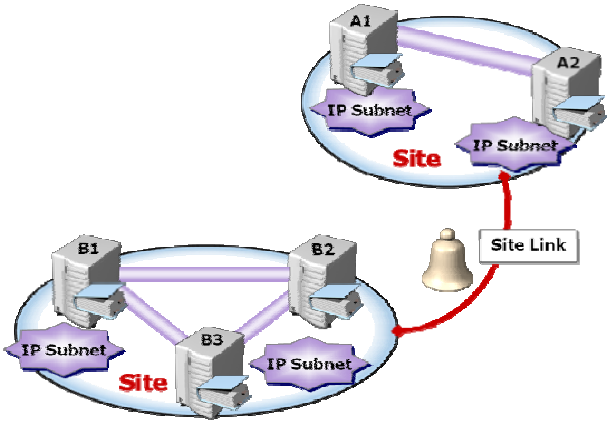
Objekt definuje určitá sada atributů, které představují něco konkrétního (například uživatel, tiskárna nebo aplikace). Atributy obsahují data popisující, co adresářový objekt identifikuje. Atribut může v závislosti na typu obsahovat jednu nebo více hodnot. Každý objekt v *Active Directory Domain Services* má jedinečnou identitu. Objekty lze přejmenovávat nebo přesouvat, ale jejich identita se nikdy nemění. Identitu udává *GUID (Globally Unique Identifier)*, který je nově vytvářeným objektům přidělován agentem adresářového systému *DSA*. Identifikátor *GUID* je uložen v atributu *objectGUID*, který je součástí každého objektu. [2, 17, 16]

2.1.4 Lokality (Site)

Síť je skupina počítačů sestavená z jedné nebo více podsítí protokolu IP. Prezentují fyzickou strukturu sítě. Proto jsou nezávislé na logických doménových strukturách a nemají spolu žádný vztah. V jedné doméně *AD DS* je možné vytvářet více sítí nebo může být pouze jedna, která bude k dispozici více doménám. [9, 16]

2.1.4.1 Replikace Lokalit

Pojmenované *Lokality (Sites)* přidružené do podsítí, kterým je nutné vytvořit plán replikace. Obvykle se nastavuje tak, že nastává alespoň každých 180 minut, 24 hodin a 7 dní v týdnu. Při omezení šířky pásma je vhodné plán upravit tak, aby měl uživatelský provoz v době špičkového zatížení sítě prioritu. V opačném případě je možné frekvenci replikací zvýšit. Ve všech případech je potřebné šířku pásma monitorovat, kvůli lepší představě o využití šířky pásma a obdobích špičkového zatížení. [12]



Obr. 5. Replikace mezi lokalitami (Site) [14]

2.1.5 Doménový řadič (Domain Controller)

Řadič domény (DC) služby *Active Directory Domain Services* je pravděpodobně nejdůležitějším typem síťového serveru v síti Windows. Tyto servery musejí být stabilní, chráněné a dostupné, aby mohly poskytovat klíčovou podporu pro adresářovou službu (např. ověřování uživatele nebo přístup ke zdrojům). Jestliže dojde ke ztrátě nebo kompromitování *DC*, následky budou kritické pro klienty, servery a aplikace, které užívají ověřování zásad skupin a adresáře protokolu *LDAP* závislých na doménových řadičích. [20, 12]

2.1.5.1 Doménový řadič jen pro čtení (Read Only Domain Controller)

Doménový řadič jen pro čtení (RODC) je určen pro umístění do prostředí s malou fyzickou bezpečností, například do pobočkových sítí. Databáze *Active Directory* na serveru *RODC* neobsahuje hashe hesel uživatelů a standardně se neukládají do mezipaměti (cache) uživatelská ověření, čímž se eliminuje offline útok hrubou silou se snahou o získání uživatelského hesla. Navíc, je možné definovat uživatele s právy správce daného *RODC* bez udělení rozšířených práv v doméně a provozovat aplikace vyžadující doménový řadič.

Jde tedy hlavně a primárně o bezpečnost. Replikace doménové databáze *AD* probíhá jen jednosměrně, směrem ze standardního *DC* na řadič *RODC*. Znamená to, že na *RODC* nelze provést žádné změny. Požadavky na změny a ověření jsou přesměrovány na „plný“ doménový řadič. Nicméně, je možné definovat skupiny uživatelů, pro které se hesla na *RODC* přeci jen v rámci replikace kopírují a *RODC* je schopen je ověřit. [23]

2.1.5.2 Flexible Single Master of Operation (FSMO)

Vyhrazený hlavní operační server má roli *FSMO (Flexible Single Master of Operation)* a má pět vyhrazených rolí:

- *Hlavní server schémat (Schema Master),*
- *Hlavní server pro pojmenování domén (Domain Naming Master),*
- *Hlavní server RID (Relative ID Master),*
- *Emulátor primárního řadiče domény (PDC Emulátor),*
- *Hlavní server infrastruktury (Infrastructure Master).*

Hlavní server schémat a *Hlavní servery pro pojmenování domén* se přiřazují pro jednotlivé doménové struktury = v jedné doménové struktuře pouze jeden *Hlavní server schémat* a jediný *Hlavní servery pro pojmenování domén*. Další tři role se přiřazují v jednotlivých doménách, ale pro každou doménu existuje pouze jediný server s danou hlavní rolí operačního serveru. [24, 12]

2.1.6 Organizační jednotka (Organizational Unit)

Organizační jednotky (OU) jsou logické kontejnery používané k uspořádání objektů v doméně. Svým nejmenším rozsahem, na kterém lze delegovat pravomoci, jsou *OU* nepostradatelné při usnadnění správy účtů pro uživatele, skupiny, počítače a taktéž pro správu ostatních prostředků, jako jsou sdílené položky a tiskárny. Přidáním *OU* k jiným *Organizačním jednotkám* se vytvoří hierarchie uvnitř domény, která je nezávislá na ostatních doménách. *OU* lze použít k:

- popisu způsobu správy prostředků a účtů,
- popisu struktury oddělení v rámci organizace,
- popisu geografických umístění obchodních jednotek,
- popisu nákladových středisek v rámci organizace.

Standardně všechny podřízené *OU* dědí oprávnění od nadřazených *OU*. [9]

Obr. 6. Hiearchie OU [13]

2.1.7 Skupina (Group)

Skupiny se využívají v procesu přidělování oprávnění podobným typům uživatelů a s tím související zjednodušení správy účtů. Pokud je uživatel členem skupiny, která má přístup k prostředku, může tento uživatel k prostředku také přistupovat. Je daleko efektivnější přiřazovat uživatele do skupin než samotná oprávnění přidávat uživatelům. [9, 14]

2.1.7.1 Typy skupin

V systému Windows Server 2008 R2 se využívají dva typy skupin:

- *Skupina zabezpečení (Security groups)* – umožňuje řídit přístup k prostředkům, mají *SID (Security Identifiers)*.
- *Distribuční skupina (Distribution groups)* – slouží pro nezabezpečené e-mailové seznamy, nemají *SID*. [12]

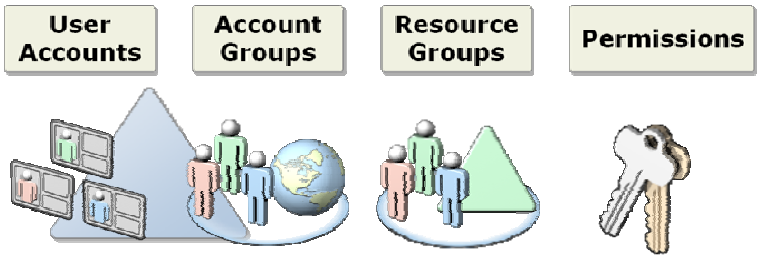
2.1.7.2 Rozsah skupin

Dále jsou skupiny rozděleny do tří typů oborů skupin:

- *Místní doménová skupina (Domain Local Group)* – poskytuje uživatelům přístup k prostředkům místní domény. Zásady přístupu do *Místní doménové skupiny* se neukládají ve službě *AD DS* a to znamená, že se nereplikují do *Globálního katalogu* - nejsou zjistitelné mimo hranice domény.
- *Globální skupina (Global Group)* – umožňují přístup k prostředkům podle jejich organizace a lze je vnořovat, aby bylo možné udělit přístup k libovolné doméně v doménové struktuře.

- *Univerzální skupina (Universal Group)* – lze je použít přes hranice domény, a proto uživatelé mohou patřit do libovolných domén a oprávnění je možné nastavit v rámci kterékoliv domény. Ukládají se do *Globálního katalogu*, a proto je nutné při každé změněně *Univerzální skupiny* změněné vlastnosti replikovat na další řadiče domény. [17, 12]

2.1.7.3 Strategie použití



Obr. 7. Strategie AGDLP [14]

Příkladem použití skupin je Strategie AGDLP:

- ***A**ccounts* – uživatelský účet,
- ***G**lobal* – Globální skupina,
- ***D**omain **L**ocal* – Místní doménová skupina,
- ***P**ermissions* – oprávnění.

Základem tohoto modelu je, že uživatelé jsou umístěni do *globálních skupin*, *globální skupiny* jsou umístěny do *lokálních doménových skupin* a *doménovým skupinám* jsou přiřazena *oprávnění* pro přístup ke zdrojům. [25]

2.1.8 Uživatel (User)

Systém *Windows Server 2008 R2* může obsahovat účty místních uživatelů nebo účty uživatelů domény. Na řadiči domény jsou místní uživatelé a skupiny zakázány. Ve službě *AD DS* účet uživatele obsahuje uživatelské jméno, heslo, skupiny, jejichž je členem a další popisné informace (jako je například telefon, adresa, dále atributy uživatele typu konfigurace zabezpečení a vzdáleného přístupu). [12, 13]

2.1.9 Počítač (Computer)

Kromě objektů pro kontejnery, skupiny a uživatele poskytuje služba *AD DS* také objekty reprezentující počítače. Pro přihlášení do domény musí existovat pojmenovaný objekt *počítač*, který se buď vytvoří automaticky, nebo manuálně (tato možnost je užitečná například tehdy, pokud chcete bezobslužně instalovat systém prostřednictví *Služby pro nasazení systému Windows*). [2, 14]

2.1.10 Tiskárna (Printer)

Prostřednictví objektů tiskárny je umožněno vytvářet nebo spravovat místní či sdílené tiskárny a tiskárny TCP/IP. [11]

2.2 Zásady skupin (Group Policy)

Zásady skupin (GPO) si lze představit tak, že se jedná o sadu pravidel aplikovatelnou v prostředí celého podniku, a to s pomocí:

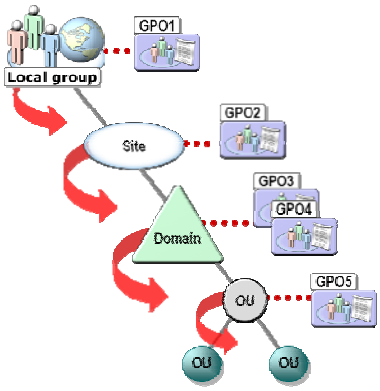
- ***Nastavení Zásad skupin*** - umožňuje řídit konfiguraci operačního systému a jeho komponent. Slouží také ke konfiguraci počítače, uživatelských skriptů, přesměrování adresářů, bezpečnosti počítače, instalaci software a k mnohým dalším účelům. Rozeznáváme tři hlavní třídy:
  - ***Nastavení Softwaru*** *(Software Setting)* – automatická instalace a upgrade.
  - ***Nastavení systému Windows*** *(Windows Settings)* – nastavení a ovládání klíčových nastavení systému Windows jak uživatelů, tak počítačů včetně zabezpečení a skriptování aj.
  - ***Šablony pro správu*** *(Administrative Templates)* – slouží ke změnám konfigurací operačního systému, komponent Windows a aplikací (např. Ovládací panely, Plocha, Síť, Sdílené složky, Tiskárny, Nabídka, Start a Hlavní panel, Systém, Součásti systému Windows).
- ***Předvolby Zásad skupin*** se uplatní při konfiguraci, nasazení a správě nastavení operačního systému a aplikací. Patří sem zdroje dat, mapované disky, proměnné prostředí, síťové disky, možnosti složky, zástupci a další. Předvolby mají dvě zásadní třídy voleb:
  - ***Nastavení systému Windows*** *(Windows Settings)* – konfigurace klíčových nastavení, pro uživatele i počítače, systému Windows – zástupců, hodnot

registrů, souborů a složek. Dále pak mapování jednotek pro uživatele a sdílení síťových složek pro počítače.

- ***Nastavení Ovládacích panelů*** *(Control Panel Settings)* – konfigurace utilit a voleb v Ovládacích panelech aj. [19, 20]

Klíčovým rozdílem mezi předvolbami a nastavením zásad je vynutitelnost. Zásady skupin přísně vynucují nastavení zásad. Naopak předvolby zásad nejsou systémem přísně vynucované. Aplikace zásad skupin spočívá ve vazbě *GPO* na součásti *AD DS*. *GPO* lze propojit s následujícími komponentami ve struktuře *AD DS*:

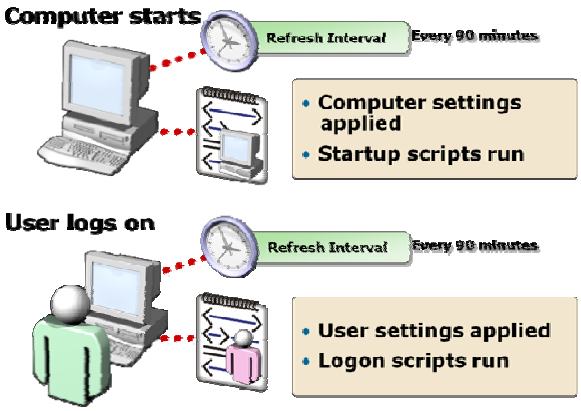
- *Lokality (Site),*
- *Domény (Domain) a*
- *Organizační jednotky (Organizational Unit).* [20, 19]



Obr. 8. Aplikace GPO [14]

V zásadách skupin rozeznáváme dvě oddělené sady zásad:

- ***Zásady počítače*** *(Computers)* – vztahují se na počítače a ukládají se v rámci *GPO* do uzlu *Konfigurace počítače (Computer Configuration)*. Zpracování zásad se aplikuje při spuštění počítače.
- ***Zásady uživatele*** *(Users)* – vztahují se na uživatele a ukládají se v rámci *GPO* do uzlu *Konfigurace uživatele (User Configuration)*. Zpracování zásad se aplikuje jako reakce na přihlášení uživatele k počítači. [20, 17]



Obr. 9. Aplikování GPO[14]

2.2.1 Správa software

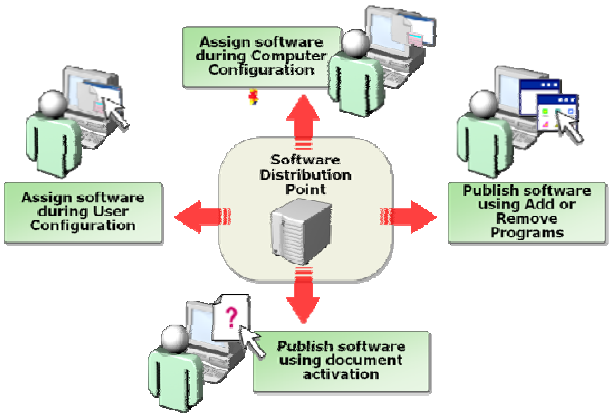
Při aplikaci doménových politik můžeme programy instalovat na *Počítač (Computer)* nebo na *Uživatele (User)*, u druhé možnosti lze předpokládat obtížné hlídání zakoupených licencí, a proto je doporučené instalovat je na počítače. Tato varianta nám umožní například „probuzení“ počítačů v noci (aplikace Wake On Line), instalaci zvolených aplikací a ráno mohou uživatelé bez jakéhokoliv zdržování začít nový nebo inovovaný software používat. [28]

Instalace software pomocí *Zásad skupin* můžeme použít tyto funkce:

- ***Publikování aplikací*** – je přiřazení SW na uživatele, její dostupnost záleží na použití, buď na síti nebo ve službě *Přidat nebo odebrat programy (Add/Remove Programs)* který si uživatel může nainstalovat ze sítě,
- ***Přiřazování aplikací*** – uživatelům nebo počítačům – automatická instalace při použití nebo při příštím spuštění PC nebo přihlášení,
- ***Instalace aplikací*** zaměřené na jednotlivé skupiny pomocí *GPO*,
- ***Výsledky stavu instalace aplikací – Group Policy Results***,
- ***Instalace aplikací*** pomocí nativních instalačních souborů (*.msi) nebo vytvořením souboru *.zap.

Přiřazení nezbytných aplikací uživatelům nebo počítačům tak, aby byli vždy dostupné. Publikací volitelných programů pro usnadnění nalezení aplikací uživatelům, právě ve chvíli, kdy je potřebují. Je nezbytné dodržovat pravidlo: nepřiřazovat ani nezveřejňovat aplikace současně uživatelů a počítačům. [2, 20]

Po zavedení SW lze zajistit, aby byl na uživatelských systémech vždy spouštěn ten správný software a jeho správná SW verze s využitím zásady *Software Restriction Policies*. [19]



Obr. 10. GPO - Instalace SW [14]

3 ROLE A SLUŽBY WINDOWS SERVER 2008 R2

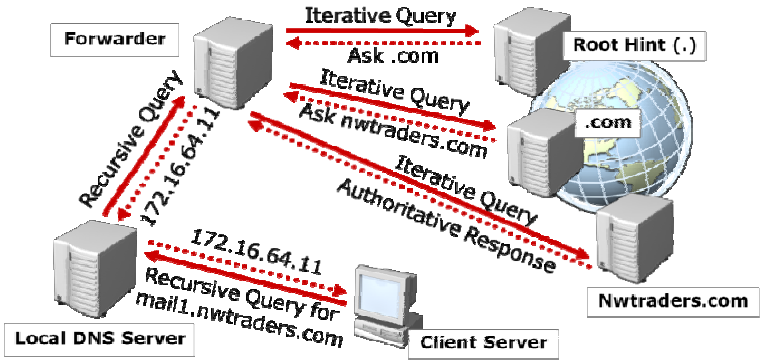
Systém *Windows Server 2008 R2* rozeznává roli serveru, službu role a funkci. Role serveru je obecné seskupení běžných funkcí, které podporují definici účelu použití serveru. Každá z těchto všeobecně definovaných rolí má k dispozici jednu nebo více služeb rolí, které jsou konkrétní funkčností a jsou dostupné pouze pro roli, pro niž slouží jako služba role. [2]

3.1 Role Domain Name System

Pro provoz role *Active Directory Domain Services* je vyžadována role *Domain Name System (DNS)*; není podmínkou používat verzi od společnosti Microsoft, ale je to doporučené z hlediska lepší provázanosti těchto rolí. [18]

Systém DNS vyžaduje klientskou i serverovou komponentu a je postaven na protokolu klient/server. Počítač, který požaduje informaci DNS je označován jako *klient DNS* a počítač, který tuto informaci poskytuje, se nazývá *server DNS*. Úkolem tohoto serveru je uchovávat databázi se záznamy DNS, odpovídat na klientské dotazy DNS a podle potřeby replikovat DNS záznamy na jiné DNS servery. Role DNS musí zajistit několik typů dotazů, včetně:

- dopředných vyhledávacích dotazů – přeložení hostitele na IP a
- zpětných vyhledávacích dotazů – překlad IP adresy na název hostitele. [30, 2]



Obr. 11. DNS – Forwarder [29]

Systém *Windows Server 2008 R2* podporuje čtyři typy zón:

- ***Standardní primární (Standard Primary)*** – všechny změny zóny se provádějí v primární zóně a její změny lze replikovat do sekundárních zón.
- ***Standardní sekundární (Standard Secondary)*** – zajišťuje redundanci pro primární zónu a vyrovnává zatížení – replikace z primární zóny pomocí přesunů zón.
- ***Integrovaná se službou Active Directory (Active Directory-Integrated)*** – integruje informace zóny ve službě *AD DS* a pomocí této služby replikuje data zóny – pouze pokud je implementována služba *AD DS*.
- ***Zóna se zakázaným inzerováním (Stub)*** – ukládá oprávněné servery DNS pro danou zónu, neobsahuje žádné informace o hostitelích v zóně. Dotazy přímo oprávněným serverům. [2, 30]

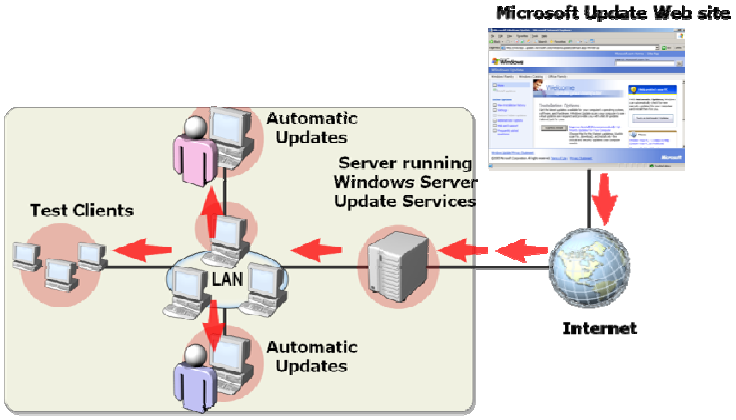
3.2 Windows Server Update Services

Microsoft Security Response Center (MSRC) je celosvětový systém k ochraně zákazníků společnosti Microsoft před zneužitím chyb zabezpečení. *MSRC* proaktivně monitoruje odhalená zranitelná místa a koordinuje činnosti vedoucí k vytvoření bezpečnostní aktualizace. Aktualizace je pak podrobena důkladnému testování z hlediska stability a kompatibility. Teprve pokud projde těmito testy, je tato aktualizace oficiálně vydána. Ke každé chybě zabezpečení je vydán bulletin zabezpečení společnosti Microsoft, který popisuje dopad této chyby, stupeň závažnosti a nejčastější dotazy související s touto aktualizací zabezpečení. [27, 26]

Windows Server Update Services patří mezi nástroje, které aktivně zabezpečují správu a distribuci aktualizací.

Celá služba se skládá ze tří komponent:

- **Microsoft Update** – web, ze kterého si WSUS server stahuje informace o aktualizacích i binární soubory potřebné pro jejich instalaci.
- **WSUS server** – serverová komponenta, která umožňuje skrze administrátorské rozhraní získávat informace o nových aktualizacích, schvalovat či odmítat aktualizace pro skupiny počítačů, reportovat jejich stav aj.
- **Automatické aktualizace** – služba začleněná do klientů Windows 2000 SP3 a vyšší, stahuje potřebné aktualizace z WSUS a iniciuje jejich aktualizaci. [26]



Obr. 12. Windows Server Update Services [29]

3.3 Zálohování

Zálohování jsou jednoduše řečeno pojistné plány, které se budou aplikovat v případě jakýchkoliv neočekávaných situací, jež mají za následek částečnou nebo úplnou ztrátu dat. V systému *Windows Server 2008 R2* je k dispozici mnoho různých řešení zálohování a obnovení, proto je vhodné při výběru zálohovacího nástroje zohlednit typ zálohy. Systém *Windows Server 2008 R2* obsahuje nástroje:

- *Zálohování serveru (Windows Server Backup)* – dovoluje vytvářet úplné, kopírovací zálohy místních i vzdálených systémů, nedovoluje vytvářet přírůstkové zálohy.
- *Stínová kopie svazku (Volume Shadow Copy Service)* – vytváří rychlé zálohy na úrovni bloků pro operační systém, soubory, složky a diskové svazky.
- *Zálohovací nástroje pro příkazový řádek* – sada nástrojů dostupná pomocí nástroje *Wbadmin* pro *Command Line*. [12, 30]

3.4 Další důležité role a služby

Vzhledem ke skutečnosti, že podstatou této práce je návrh implementace *AD DS*, jsou zde zahrnuty role a služby, které jsou nezbytné či doporučené. Na druhou stranu by bylo neomluvitelné alespoň ve zkratce nezmínit některé další neméně důležité role a služby:

- ***Souborová služba*** *(File Server)* – poskytuje klíčové služby pro správu souborů, způsob jakým jsou soubory zpřístupněny a replikovány po síti.

- ***Tiskové služby*** *(Print Services)* – správa tiskáren a ovladačů tisku.
- ***Terminálová služba*** *(Terminal Services)* – spouštění aplikací systému Windows nainstalované na vzdáleném serveru.
- ***Webový server (IIS)*** *(Web Server IIS)* – hostuje weby a webové aplikace.
- ***Služba pro nasazení systému Windows*** *(Windows Deployment Services – WDS)* – zavádění počítačů se systémem Windows do podniku.
- ***Windows SharePoint Services*** – týmová spolupráce založená na propojení osob a informací.
- ***NAP*** *(Network Access Protection)* – zlepšení zabezpečení sítě.
- ***DHCP*** *(Dynamic Host Configuration Protocol)* – centralizovaná kontrola nad adresováním protokolu IP.
- ***AD RMS*** *(Active Directory Rights Management Services)* – poskytuje řízený přístup k chráněným e-mailům, dokumentům, webovým stránkám v intranetu a dalším typům souborů. [2, 12]

II. PRAKTICKÁ ČÁST

4 POPIS SOUČASNÉHO STAVU

V následujících kapitolách je popsán stávající stav IT infrastruktury subjektů UTB Zlín. Organizační členění celé této infrastruktury je rozděleno na část centrální – Univerzitní centrum (U13), dále pak podle jednotlivých fakult a lokací (dálen jen subjekty), které jsou připojeny k U13 pomocí optických tras. Každý ze subjektů si IT infrastrukturu spravuje sám za podpory pověřených pracovníků fakulty a U13 nabízí globální služby, které mohou být využívány při splnění předem daných podmínek.

4.1 Síťová architektura

Převážná část subjektů univerzity je soustředěna na území města Zlín a jsou propojeny technologií optických tras (nenasvícené – GigabitEthernet), které přímo spadají pod správu UTB. Další subjekty jako například detašované pracoviště Uherské Hradiště má pronajatou optickou linku (GigabitEthernet) zajištěnou sdružením CESNET.

Propojení aktivních prvků ve fakultních sítích zprostředkovává strukturovaná kabeláž (FastEthernet 10/100Base TX).

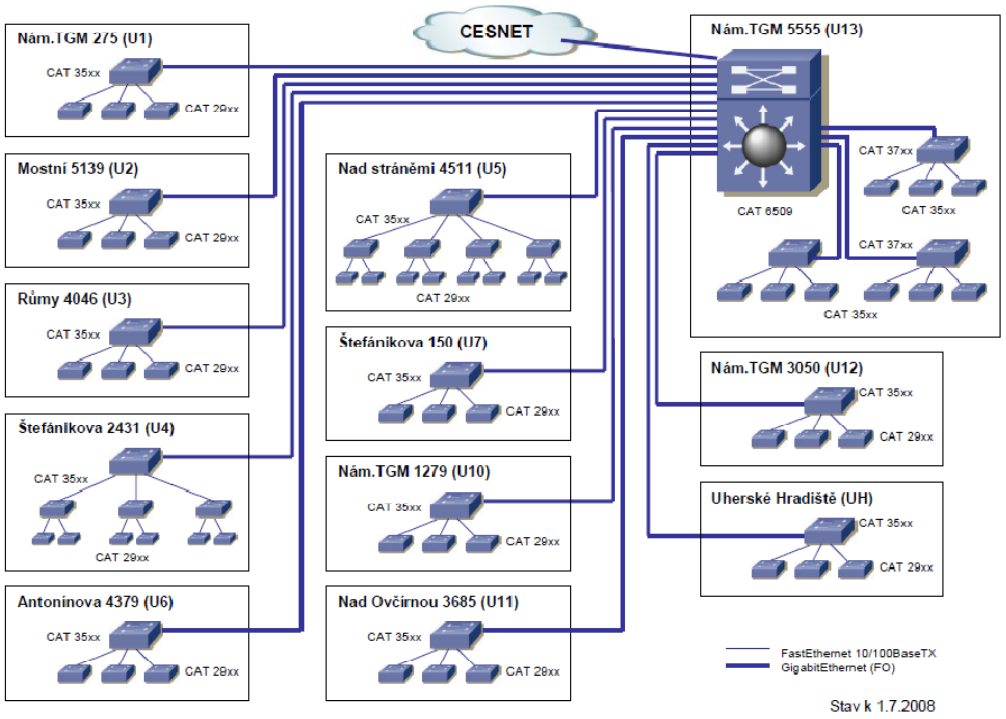
Na základě těchto informací lze tedy považovat vzájemnou konektivitu za propojení v rámci sítě LAN (Local Area Network).

4.2 IP adresní plán

Adresní plán sítě vychází z rozdělení na podsítě daným prostorovým a funkčním členěním. Převážná většina subjektů používá interní IP adresy z rozsahu 10.x.x.x, ostatní subjekty a servery mají přidělenou veřejnou IP adresu; do této kategorie spadají i služby, které pro svůj bezproblémový chod vyžadují taktéž veřejnou IP adresu.

4.2.1 IP adresace FAI

- **síť**: 10.5.0.0/24
- **DNS server**: 195.178.88.66
- **gateway**: 10.5.0.1
- **broadcast**: 10.5.0.255



Obr. 13. UTB Zlín - Blokové schéma IP sítě a aktivních prvků [zdroj UTB]

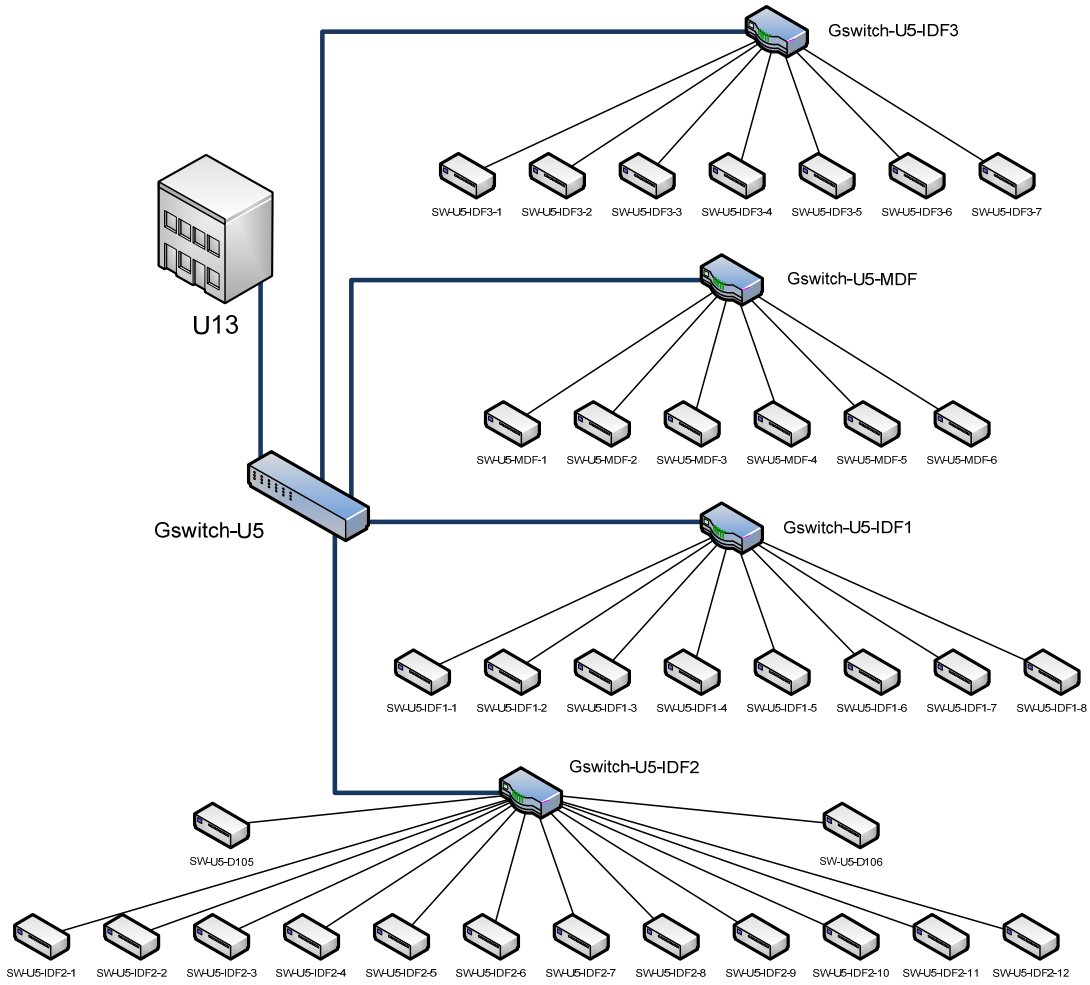
4.3 Rozdělení aktivních prvků U5 (FAI)

Switch Cisco Catalyst 3500 subjektu U5 je propojen páteřní optickou trasou s U13 (GigabitEthernet). Vzhledem k rozloze FAI, byla vytvořena síť čtyř interních páteřních optických propojení rozvedených po budově (GigabitEthernet) ukončených v Cisco Catalyst 3550 nebo 3560. Dále je rozvedena strukturovaná kabeláž k aktivním prvkům Cisco Catalyst 2950, umístěných v jednotlivých předem vybraných lokalitách, ke kterým jsou připojena jednotlivá koncová zařízení (PC, tiskárny aj.).

Tab. 2. Aktivní prvky U5

IP adresa	Host name	Vlastník	Místnost
10.5.0.6	Gswitch-U5-MDF	Cisco Catalyst 3560G-48PS	U5 / A206
10.5.0.7	Gswitch-U5-IDF1	Cisco Catalyst 3550-24	U5 / B106
10.5.0.8	Gswitch-U5-IDF2	Cisco Catalyst 3550-24	U5 / C313
10.5.0.9	Gswitch-U5-IDF3	Cisco Catalyst 3550-24	U5 / A211
10.5.0.12	SW-U5-MDF-2	Cisco Catalyst 2950-24	U5 / A206
10.5.0.13	SW-U5-MDF-3	Cisco Catalyst 2950-24	U5 / A206

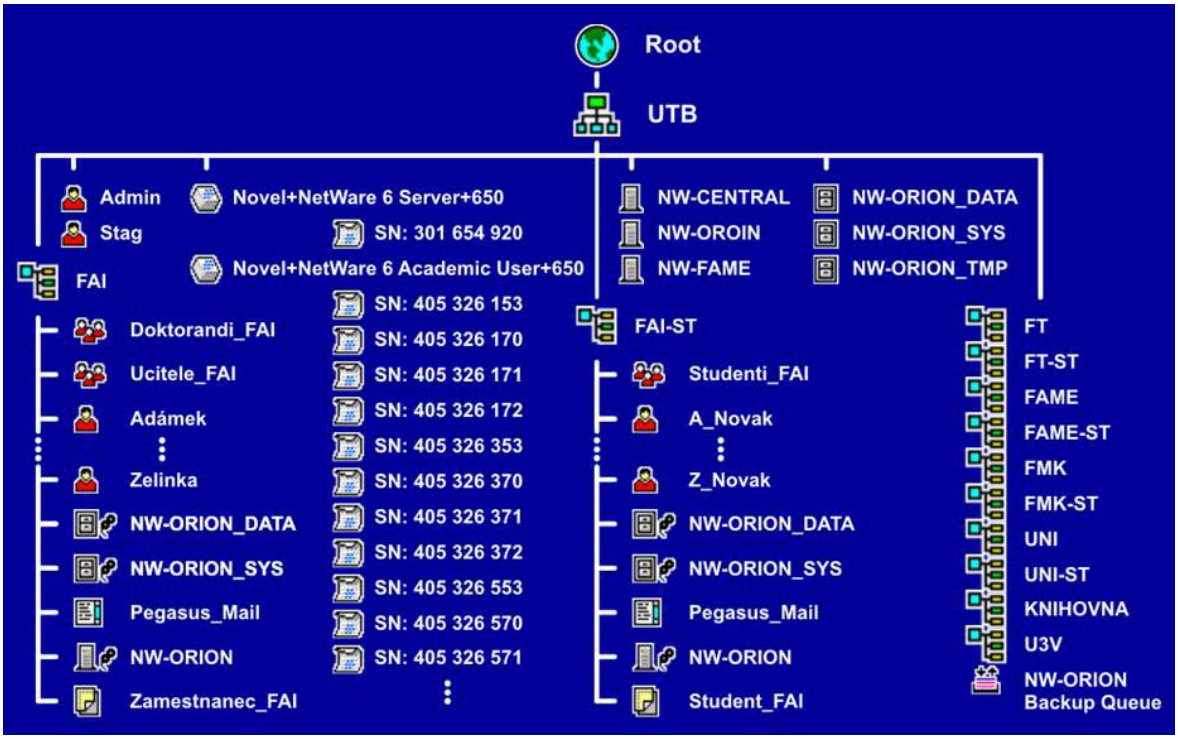
IP adresa	Host name	Vlastník	Místnost
10.5.0.14	SW-U5-MDF-4	Cisco Catalyst 2950-24	U5 / A206
10.5.0.15	SW-U5-MDF-5	Cisco Catalyst 2950-24	U5 / A206
10.5.0.16	SW-U5-MDF-6	Cisco Catalyst 2950-24	U5 / A206
10.5.0.22	SW-U5-IDF1-2	Cisco Catalyst 2950-24	U5 / B106
10.5.0.23	SW-U5-IDF1-3	Cisco Catalyst 2950-24	U5 / B106
10.5.0.24	SW-U5-IDF1-4	Cisco Catalyst 2950-24	U5 / B106
10.5.0.25	SW-U5-IDF1-5	Cisco Catalyst 2950-24	U5 / B106
10.5.0.26	SW-U5-IDF1-6	Cisco Catalyst 2950-24	U5 / B106
10.5.0.27	SW-U5-IDF1-7	Cisco Catalyst 2950-24	U5 / B106
10.5.0.28	SW-U5-IDF1-8	Cisco Catalyst 2950-24	U5 / B106
10.5.0.31	SW-U5-IDF2-1	Cisco Catalyst 2950-24	U5 / C313
10.5.0.32	SW-U5-IDF2-2	Cisco Catalyst 2950-24	U5 / C313
10.5.0.33	SW-U5-IDF2-3	Cisco Catalyst 2950-24	U5 / C313
10.5.0.34	SW-U5-IDF2-4	Cisco Catalyst 2950-24	U5 / C313
10.5.0.35	SW-U5-IDF2-5	Cisco Catalyst 2950-24	U5 / C313
10.5.0.36	SW-U5-IDF2-6	Cisco Catalyst 2950-24	U5 / C313
10.5.0.37	SW-U5-IDF2-7	Cisco Catalyst 2950-24	U5 / C313
10.5.0.38	SW-U5-IDF2-8	Cisco Catalyst 2950-24	U5 / C313
10.5.0.39	SW-U5-IDF2-9	Cisco Catalyst 2950-24	U5 / C313
10.5.0.40	SW-U5-IDF2-10	Cisco Catalyst 2950-24	U5 / C313
10.5.0.41	SW-U5-IDF2-11	Cisco Catalyst 2950-24	U5 / C313
10.5.0.42	SW-U5-IDF2-12	Cisco Catalyst 2950-24	U5 / C313
10.5.0.61	SW-U5-D105	Cisco Catalyst 2950T-24	U5 / D105
10.5.0.62	SW-U5-D106	Cisco Catalyst 2950T-24	U5 / D106
10.5.0.51	SW-U5-IDF3-1	Cisco Catalyst 2950-24	U5 / A211
10.5.0.52	SW-U5-IDF3-2	Cisco Catalyst 2950-24	U5 / A211
10.5.0.53	SW-U5-IDF3-3	Cisco Catalyst 2950-24	U5 / A211
10.5.0.54	SW-U5-IDF3-4	Cisco Catalyst 2950-24	U5 / A211
10.5.0.55	SW-U5-IDF3-5	Cisco Catalyst 2950-24	U5 / A211
10.5.0.56	SW-U5-IDF3-6	Cisco Catalyst 2950-24	U5 / A211
10.5.0.57	SW-U5-IDF3-7	Cisco Catalyst 2950-24	U5 / A211



Obr. 14. Aktivní prvky U5

4.4 Operační systém

V současné době je na File Serverech nasazen síťový operační systém Novel Netware 6.5, který je umístěn na serverech **nw-central**, **nw-orion**, **nw-fame**. Umožňuje centrálně spravovat uživatelské účty a svazky disků.



Obr. 15. Struktura NDS UTB Zlín + licence [zdroj: UTB]

4.5 Síťové služby

4.5.1 DNS

Nyní existuje jmenný prostor utb.cz. Jde o distribuované DNS servery postavené na serverech LINUX Debian . Primární DNS server je umístěn v Univerzitním centru (U13), sekundární DNS server je provozován na serveru sdružení CESNET v Praze. Definují se A záznamy IPv4. Tyto DNS servery podporují provoz dalších domén 2. řádu sloužících pro různé akademické projekty v rámci UTB.

4.5.2 WINS

V současné době se tato síťová služba nevyužívá.

4.5.3 Network Time Protocol

V síti UTB je definován jeden NTP (Network Time Protocol) server ntp.utb.cz, který je synchronizován s NTP serverem sdružení CESNET.

4.5.4 Dynamic Host Configuration Protocol

V současné době jedna část síťových zařízení obsahuje statické síťové informace a druhé části síťových zařízení jsou tyto přidělovány serverem DHCP (Dynamic Host Configuration Protocol) na operačním systému Linuxu Debian. V rámci pilotního projektu byl v roce 2009 v univerzitní síti nasazen systém ARPMon od společnosti Novicom, jehož součástí je i DHCP, na které bude tato služba postupně migrována ze stávajícího operačního systému.

4.5.5 PKI

V současné době se tato síťová služba nevyužívá.

4.5.6 WSUS

V současné době se tato síťová služba nevyužívá.

4.6 Ostatní služby

4.6.1 Centrální správa antiviru

V současné době se tato síťová služba nevyužívá na úrovni univerzity. Každý subjekt řeší individuálně svou antivirovou ochranu a má nasazena různá řešení. Konfigurace vychází ze zkušeností jednotlivých pověřených pracovníků a požadavků uživatelů.

4.6.2 Elektronická pošta

Správu e-mailů zajišťuje e-mailový server Postfix, který veškerou příchozí poštu kontroluje na přítomnost virů (NOD32) a spamu (SpamAssassin) a dále ji předává dalším serverům, kde jsou uloženy e-mailové schránky uživatelů. Stejný server zajišťuje odesílání veškeré pošty z univerzity smtp.utb.cz. Samozřejmostí je podpora protokolů POP3 a IMAP, z čehož vyplývá, že pro přístup k e-mailu je možné použít libovolného klienta podporujícího tyto protokoly nebo lze použít webového klienta SquirrelMail na adrese webmail.utb.cz.

4.6.3 Ostatní systémy

Další zásadní systémy používané v UTB Zlín jsou SAP, STAG, Moodle, ALEPH (knihovní systém), databázové systémy - menzovní systém, přístupový systém, systém evidence publikací, reprografické služby a portál Websphere.

4.7 Uživatelé, počítače a lokální administrátoři

Vzhledem k zaměření organizace jsou uživatelé rozděleni na studenty a zaměstnance jednotlivých subjektů univerzity. Do skupiny zaměstnanců dále pak patří lokální a síťoví administrátoři.

Tab. 3. Přehled zaměstnaců a studentů

Subjekt	Studenti	Zaměstnanci
FAI	1700	103
FAME	3420	115
FHS	1860	79
FMK	1210	76
FT	2250	222
Rektorát	-	117
UNI	-	26
KMZ	-	58

[Zdroj: UTB]

U zaměstnanců předpokládáme denní používání počítačů při zpracování agendy související s chodem univerzity, naproti tomu studenti vstupují do systému například v učebnách nebo v knihovně.

Pro následný návrh byla potřeba vymezit stav PC na jednotlivých subjektech pro definování návrhu *Active Directory Domain Services*:

- méně než 10 počítačů U6, U7 a U12,
- více jak 50 počítačů se nachází na U1, U2, U4, U5, U10, U11, detašované pracoviště UH a U13,
- na žádném subjektu není více jak 2000 počítačů.

Určení *Lokální administrátoři* udržují chod IT technologií na jednotlivých subjektech, přičemž může být jejich kompetence rozšířena například:

- u subjektu U3 – lokální administrátor z U11 a U5,
- u subjektu U10 – lokální administrátor z U2 (FHS) a
- subjekty U6, U7 a U12 – společný lokální administrátor.

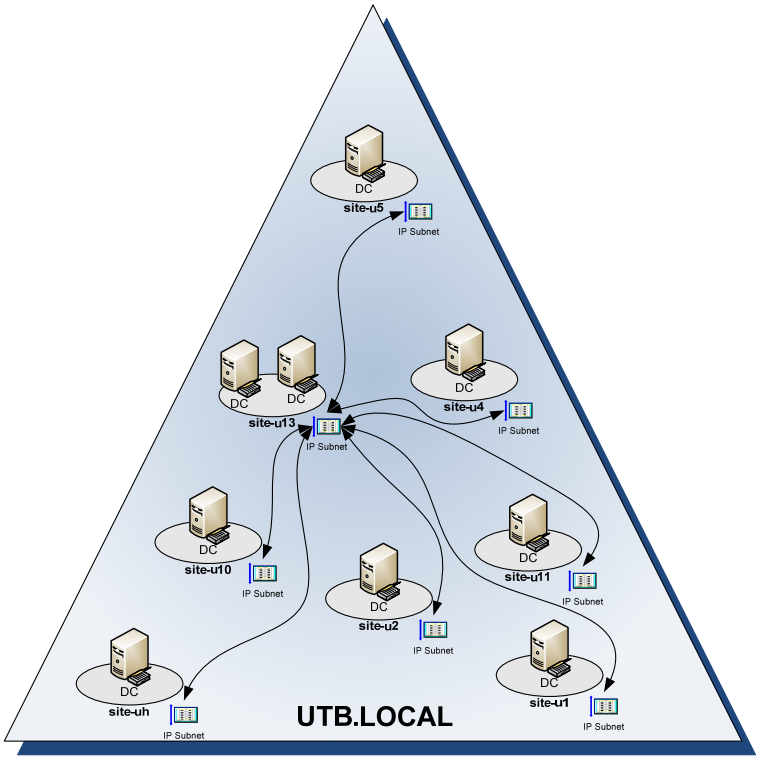
5 DESIGN ACTIVE DIRECTORY DOMAIN SERVICES

Design je vytvořen pro prostředí organizace Univerzity Tomáše Bati ve Zlíně na základě analýzy, návrhů autora a podnětů vedoucího této práce.

Základní myšlenkou designu je vytvoření takové struktury, která efektivně zpřístupňuje adresářové informační zdroje, aplikace a služby koncovým uživatelům prostřednictvím jednoho přihlášení. Řešení je v úzkém vztahu s bezpečnostními prvky koordinovanými z jednoho místa pro oblast rozsáhle sítě univerzity.

5.1 Doménová struktura

V rámci návrhu doménové struktury je upuštěno od *více domenové struktury* i *doménového forestu* a je zvolena *jedna doménová architektura* s ohledem na velkou migraci studentů mezi subjekty s předpokladem stejné základní bezpečnostní a přístupové politiky pro celou univerzitu.



Obr. 16. Návrh doménové struktury

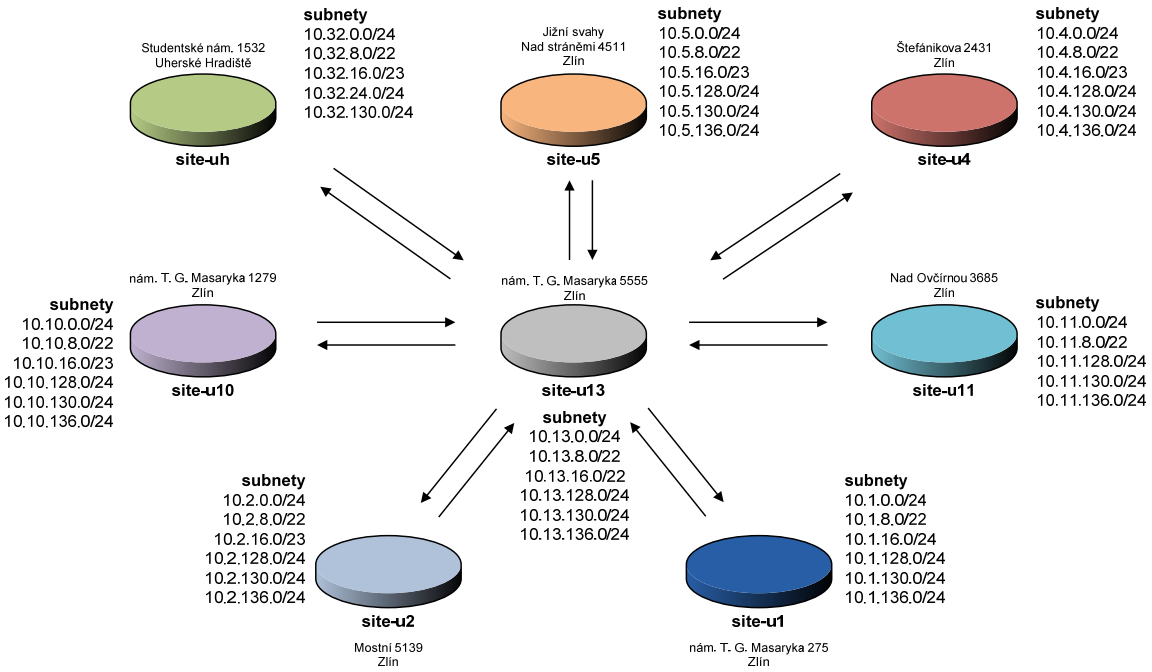
Jediná doména s názvem ***utb.local*** zajišťuje doménové prostředí univerzity, která je spravována devíti *Doménovými řadiči (Domain Controler, DC)* z toho jsou dva hlavní,

umístěné v U13 (site-u13) a v dalších *Lokalitách (Site)* po jednom DC. Replikací všech singulárních *Lokalit (Site)* docílíme totožné informace na všech *Doménových řadičích (Domain Controler)*. Doména je dále rozvržena do *Organizačních jednotek (Organizational Unit, OU)* a ty jsou použity pro delegování administrátorských práv a nastavování jednotlivých *Zásad skupin (Group Policy, GPO)*.

5.2 Rozdělení síťové infrastruktury do Lokalit (Site)

Tato práce popisuje *Lokality (Site)* jako pojmenovaný objekt v *AD DS*, obsahující referenci na *Podsítě (Subnet)*, které administrativně zahrnují soubor IP adres do jednoho celku v rámci *Active Directory Domain Services*. Vzhledem k filozofii Microsoft Windows Server musí být v každé *Lokalitě* umístěn minimálně jeden *Doménový řadič*, který mimo doporučených serverových rolí může obsahovat *Globální katalog*.

Rozdělení do *Lokalit* v rámci LAN UTB Zlín, zohledňuje počty lokálních počítačů a potencionálních uživatelů dle kritérií, které přímo souvisejí s umísťováním *Doménových řadičů* – viz kapitola 5.3.



Obr. 17. Návrh Lokalit (Site) a Podsítí (Subnet)

Návrh *Podsítí* je ponechán dle stávávajícího rozdělení vnitřních IP adres a je umístěn do pojmenovaných *Lokalit*. V Příloze I. jsou zahrnuty jak názvy *Lokalit* a jejich umístění, tak i použitý adresní blok.

5.2.1 Nastavení replikací

Návrh řeší dva druhy replikací, které nabízí Microsoft *Windovs Server 2008 R2,* a to:

- uvnitř *Lokality* a
- mezi *Lokalitami*.

Lokalita site-u13 obsahuje dva vyhrazené *Doménové řadiče*, jejich nekomprimovaná data jsou automaticky replikována procesem *Knowledge Consistency Checker (KCC)* uvnitř *Lokalit*. U ostatních *site-links* (replikace mezi *Sites*) je přihlédnuto k efektivitě a uvolnění síťových prostředků, proto jsou replikovány automaticky dle plánu a jejich data jsou komprimována.

Tab. 4. Plán replikací

site-links	replikace	čas replikace	cost
site-u13	KCC	default	-
site-u13 – site-u5	automatická	60 minut	20
site-u13 – site-u4	automatická	60 minut	20
site-u13 – site-u10	automatická	60 minut	20
site-u13 – site-u11	automatická	60 minut	20
site-u13 – site-u1	automatická	60 minut	20
site-u13 – site-u2	automatická	60 minut	20
site-u13 – site-uh	automatická	default	40

Na základě zkušeností s provozem *AD DS* je možné tento návrh změnit navýšením stávajících replikací o nové směry nebo upřesněním plánu a ohodnocením linky.

5.3 Doménové řadiče (Domain Controllers) - rozmístění

V doméně ***utb.local*** jsou navrženy *Doménové řadiče* jednak z důvodu účinného využití konektivity LAN a dále pak, při nefunkčnosti propojení mezi *Lokalitami* musejí zajistit přihlášení do místní sítě v rámci příslušného DC.

Kritéria návrhu DC:

- pro 20 – 2000 uživatelů je společností Microsoft doporučeno umístit *Doménový řadič*, který je umístěn do objektu *Lokality*,
- v lokalitě U13 je hlavní systém, který musí být redundantní,
- vzhledem k zaměření organizace byl místo počtu uživatelů použit počet počítačů v rámci subjektu a
- nebyl brán zřetel na IT vybavení v osobním vlastnictví studentů, u kterých se nepředpokládá připojení k Doméně.

Lokality U6, U7 a U12 mají méně než 10 počítačů, proto jsou propojeny přímo na DC umístěné v site-u13.

Tab. 5. Role vyhrazených serveru

Site	Domain name	DC name	Role	Globální katalog
site-u1	utb.local	U1-DC01	DC, DNS	ano
site-u2	utb.local	U2-DC01	DC, DNS	ano
site-u4	utb.local	U4-DC01	DC, DNS	ano
site-u5	utb.local	U5-DC01	DC, DNS	ano
site-u10	utb.local	U10-DC01	DC, DNS	ano
site-u11	utb.local	U11-DC01	DC, DNS	ano
site-u13	utb.local	U13-DC01	DC, DNS, NTP	ano
site-u13	utb.local	U13-DC02	DC, DNS	ano
site-uh	utb.local	UH-DC01	DC, DNS	ano

5.4 Globální katalog (Global Catalog)

Funkce Globálního katalogu, vzhledem k jednodoménové struktuře, je aktivní na všech *Doménových řadičích (Domain Controllers)* v doménovém prostoru UTB Zlín.

5.5 Flexible Single Master Operations role

Server **U13-DC01** je určen jako jediný autoritativní server - *hlavní operační server* (Operations Master) a plní roli Flexible Single Master Operations (FSMO).

5.6 Jmenné konvence

Jedním ze základních předpokladů úspěšné implementace *Active Directory Domain Services* jsou jmenné konvence, jak z hlediska snadného dohledávání lokalit, serverů, počítačů nebo uživatelů, tak struktury celého doménového prostoru UTB Zlín. Nevhodně zvoleným pojmenováním mohou v budoucnosti vzniknout situace, které budou působit chaoticky a nesystémově. Jediným úspěšným řešením je striktní dodržování vybrané terminologie názvů.

5.6.1 Doména

Definice jmenné konvence domény vychází z již daných pravidel pojmenování a všeobecně se vymezují tři tvary:

1. **název-subjektu.cz** – středoevropská,
2. **název-subjektu.local** – německá,
3. **int.nazev-subjektu** – americká.

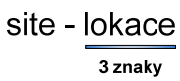
Nejpoužívanějším řešením v České republice jsou jmenné konvence středoevropské, které s sebou nesou úskalí při konfiguraci a správě role *DNS (Domain Name System)*, proto je záměrně oddělena interní doména od externí s použitím německé konvence. Název domény je ***utb.local***. Praktickou výhodou této jmenné konvence je nemožnost kolidování externích subdomén s interní doménovou strukturou, která souvisí s externím pojmenováním fakult a projektů (příklad: fai.utb.cz).

5.6.2 Doménové řadiče (Domain Controller)

Jmenné konvence u *DC* budou vycházet z pojmenování serverů, které jsou podrobně popsané níže v kapitole Servery. V případě, že daný server ve své konfiguraci zahrnuje více rolí a jednou z nich je *Doménový řadič*, bude se tato role upřednostňovat při přidělování jmenných konvencí jednotlivým serverům.

5.6.3 Lokace (Site)

Podkladem pro vytvoření replikačních cest jsou jasně identifikovatelné *Lokace*, proto byla zvolena velmi jednoduchá strategie vytváření jmen.



Obr. 18. Struktura Lokace (Site)

Kde:

- **site** = pevná část názvu, označující *Site,*
- **lokace** = volitelná část názvu - označení lokality, kde je *Site* umístěna (3 znaky).

Příklad: *site-u5* nebo *site-u1*

5.6.4 Organizační jednotky (Organization units)

Organizační jednotky (OU) jsou specifické neměnné názvy, při jejichž vytváření se bude vycházet z organizační struktury UTB, její funkce a lokality.

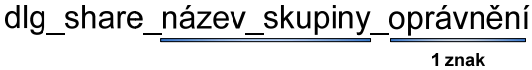
Příklad: *OU FAI*, *OU IT Admins*, *OU FAI PC*

5.6.5 Skupiny (Groups)

Pro řízení přístupu ke zdrojům budou nadefinována přesná pravidla využívající skupinu zabezpečení v *Active Directory Domain Services*. Použitím vícenásobného seskupení objektů do logických celků lze zdroje velmi jednoduše administrovat.

5.6.5.1 Lokální skupina (Local Group)

Lokální skupiny budou nastaveny pro určitý zdroj a přiřadí příslušné *oprávnění (Permission)*, které poskytne autorizaci *číst (Read)* nebo *psát (Write)* v rámci domény.



Obr. 19. Struktura Lokální skupina

Kde:

- **dlg_share** = pevná část názvu, která určuje druh skupiny,
- **název_skupiny** = transparentní název skupiny,

- **oprávnění** = přiřazení oprávnění (1 znak)
    - **r** (Read) = číst,
    - **w** (Write) = psát,

Příklad: *dlg_share_ABAUI_r* nebo *dlg_share_ABAUI_rw* = přístup do adresáře ABAUI

5.6.5.2 Globální skupina (Global Group)

Jmenné konvence budou určeny dle organizační struktury, lokace nebo právě probíhajícího školního projektu. Autorizace pro skupiny a účty z jakékoliv domény uvnitř doménového stromu nebo lesa.

Příklad: *Studijni oddeleni*, *Implementace AD*

5.6.6 Objekty skupinové politiky (Group Policy Objects)

Transparentní označení *objektů skupinových politik* je založena na funkci objektu a jeho popisu.

Funkce objektu_Popis objektu_Policy
dle potřeby dle potřeby

Obr. 20. Struktura Objekty skupinové politiky

Kde:

- **Funkce objektu –** definice funkce GPO
    - **Restricted, Allowed, TurnOn, TurnOff,**
- **Popis objektu** – jasné popsání funkce GPO,
- **Policy** – pevná část názvu.

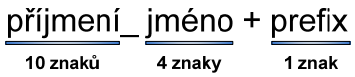
Příklad: *Restricted_CommandLine_Policy* nebo *Allowed_Proxy_Policy*

5.6.7 Uživatelé (Users)

Přihlašovací jméno (Logon name) musí být v celé doméně jedinečné, nerozlišují se malá a velké písmena obsahující a-z, A-Z, 0-9 a nemůže být delší než 20 znaků.

5.6.7.1 Zaměstnanci a doktorandi

Struktura pojmenování jednotlivých zaměstnanců a doktorandů vychází z jejich jména a příjmení. V případě duplicit bude použit prefix.



Obr. 21. Struktura zaměstnanci a doktorandi

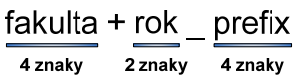
Kde:

- **příjmení** = příjmení uživatele (10 znaků),
- **jméno** = jméno uživatele (4 znaky),
- **prefix** = číselná hodnota odlišující duplicity (1 znak).

Příklad: *novakova_eva*, *novak_mart2*

5.6.7.2 Studenti

Přihlašovací jména studentů mohou mít stejnou strukturu jako v kapitole 0, ale bude mimořádně obtížné řešit duplicitní názvy nemalého množství studentů UTB Zlín. Proto byla zvolena jiná strategie - cílem bylo zformovat takové ID, které se bude lehce vytvářet a bude předcházet vzniku duplicit.



Obr. 22. Struktura studenti

Kde:

- **fakulta** = název fakulty, pod kterou student spadá (4 znaky),
- **rok** = rok přijetí do školy (2 znaky),
- **prefix** = po sobě jdoucí číselná řada (4 znaky).

Příklad: *fai09_0045*, *fame10_0789*

5.6.8 Servery a počítače

Jména serverů a počítačů musejí být jedinečná v doménové struktuře a mohou obsahovat malá i velká písmena v alfanumerickém formátu (a-z, A-Z, 0-9). Délka jména by neměla přesáhnout 15 znaků.

5.6.8.1 Servery

Pojmenování bude dle následné konvence:

lokace (4 znaky) + s – funkce serveru (3 znaky) + prefix (2 znaky)

Obr. 23. Struktura servery

Kde:

- **lokace** = fakulta, kde je server umístěný (4 znaky),
- **s** = typ IT zařízení, v tomto případě server,
- **funkce serveru** = jakou primární funkci bude server zastávat (3 znaky),
- **prefix** = číselná hodnota odlišující duplicity (2 znaky).

Příklad: *U13-DC01*, *U1-DNS01*

Tab. 6. Příklady funkce serverů

Funkce	Kód funkce
Domain controller	DC
SQL server	SQL
Proxy server	PRX
Web server	WEB
Print server	PRT
File server	FS
Terminal server	TS
Mail server	MSG

5.6.8.2 Počítače

Pojmenování bude dle následné konvence:

lokace (4 znaky) + typ IT (1 znak) - příjmení uživatele (prvních 5 znaků) + číslo kanceláře (4 znaky)

Obr. 24. Struktura počítače

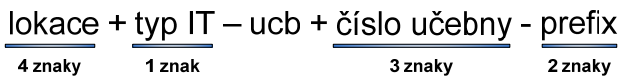
Kde:

- **lokace** = fakulta, kde je počítač umístěný (4 znaky),
- **typ IT** = druh počítače (1 znak)
    - **p** = počítač,
    - **n** = notebook,
- **příjmení uživatele** (prvních 5 znaků),
- **číslo kanceláře** = číslo kanceláře, kde je umístěno zařízení (4 znaky).

Příklad: *u1p-novak234*, *u5n-krejc23*

5.6.8.3 Počítače učebny

Pojmenování bude dle následné konvence:



Obr. 25. Struktura počítače učebny

Kde:

- **lokace** = fakulta, kde je počítač umístěný (4 znaky),
- **typ IT** = druh počítače (1 znak)
    - **p** = počítač,
    - **n** = notebook,
- **ucb =** počítač na učebně,
- **číslo učebny** (3 znaky),
- **prefix** = číselná hodnota odlišující duplicity (2 znaky).

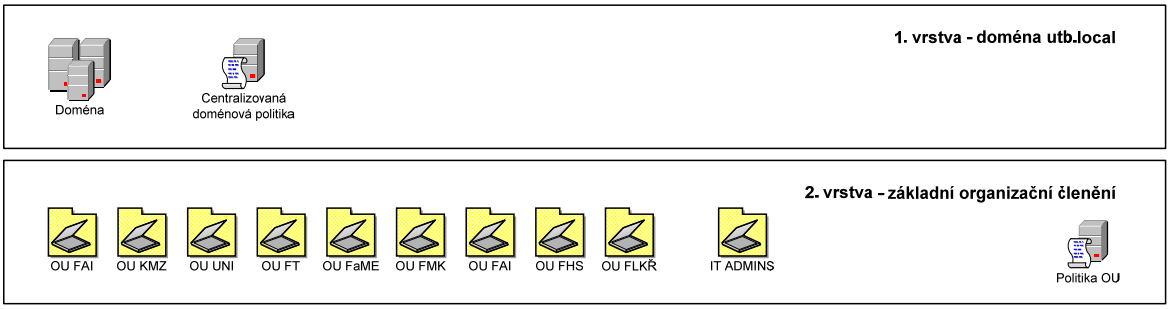
Příklad: *u5p-ucb234-01*, *u13p-ucb23-12*

6 DESIGN SKUPINOVÉ POLITIKY (GROUP POLICY)

Hierarchické členění návrhu organizačních jednotek UTB ve Zlíně přímo ovlivňuje způsob, jakým je doména spravována pomocí *Skupinových politik (Group Policy, GPO)* a samozřejmě poskytuje možnost delegování správy.

6.1 Základní členění Organizačních jednotek univerzity

Pro základní rozložení *Organizačních jednotek (Organizational Unit, OU)* na Univerzitě Tomáše Bati ve Zlíně se jevilo jako nejvhodnější centralizované řízení definované dle uspořádání:



Obr. 26. Organizační jednotky UTB Zlín

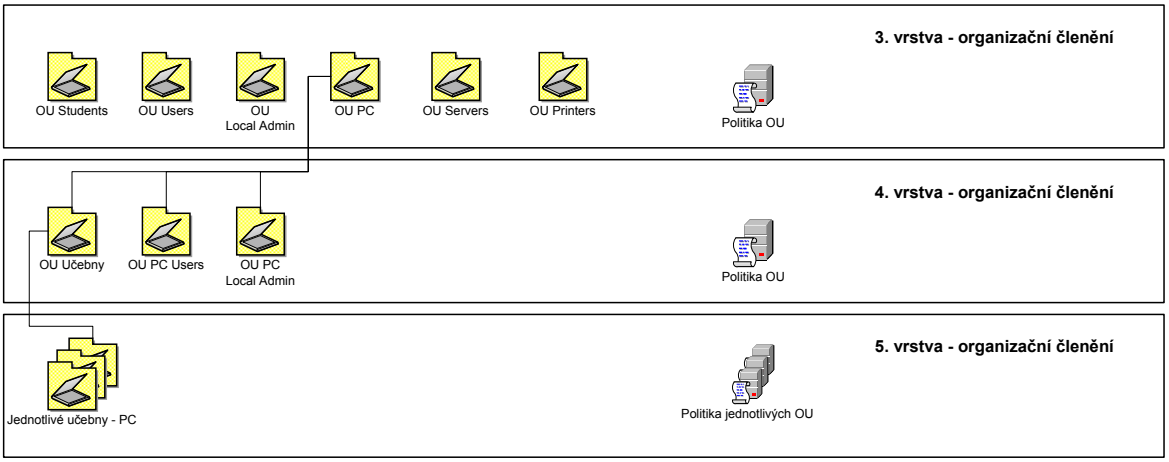
- **1. vrstva** – root doména,
- **2. vrstva** – výchozí *OU* - dělení do logických celků se zaměřením na fakulty a IT administrátory těchto bloků.

6.2 Organizační členění Fakulty aplikované informatiky

Principiálně byl návrh postaven na skutečnosti, že jednotlivé ústavy fakulty spadají pod správní strukturu *Organizační jednotky* Fakulty aplikované informatiky a z toho vyplývá, že jejich řízení může být částečně decentralizované, ovšem závislé na centrálních politikách nastavených na doménové úrovni 1. vrstvy.

Tento návrh zajišťuje autonomii nad objekty, transparentní řízení objektů, efektivní využití *Zásad skupin* a měl by odolat reorganizaci fakulty, i když se předpokládá, že na základě zkušeností s používání *Active Directory Group Services* dozná tento návrh změn.

Proto je nezbytná a doporučená pečlivá dokumentace všech budoucích rozšíření a upřesnění *OU*.



Obr. 27. Organizační jednotky FAI

- **3. vrstva** – rozlišuje *OU* všech studentů (*OU Students*), zaměstnanců (*OU Users*), lokálních správců počítačů (*OU Local Admin*), serverů (*OU Servers*), sdílených tiskáren (*OU Printers*) a počítačových stanic (*OU PC*),
- **4. vrstva** – zajišťuje správu počítačů lokálních administrátorů (*OU PC Local Admin*), zaměstnanců (*OU PC Users*) a učeben (*OU Učebny*),
- **5. vrstva** – seskupuje všechny počítačové učebny na FAI

Design členění Organizačních jednotek pro Fakultu aplikované informatiky lze s mírnými změnami aplikovat na ostatní fakulty.

6.3 Strategie Skupin (Groups)

Cílem návrhu *Skupin* je zjednodušení správy, a to takovým způsobem, že administrátoři přiřazují práva a oprávnění skupinám nikoliv jednotlivým uživatelům.

Při použití jediné domény ***utb.local*** je zbytečné aplikovat *Univerzální skupinu (Universal group)* a z tohoto důvodu byla použita strategie *AGDLP (Accounts, Global, Domain Local, Permissions)*.

- **Uživatelské účty** (*Accounts*),
- **Globální rozsah** (*Global*) – strukturu určuje organizační struktura, lokace, aj.

- **Místní doménový rozsah** (*Domain Local*) – strukturu určují zdroje (sdílené složky, tiskárny aj.),
- **Oprávnění** (*Permissions*) – uplatněné oprávnění.

Názvy skupin musejí být okamžitě rozpoznatelné - jasně říkat, za jakým účelem byly dotyčné skupiny vytvořeny, a to i s ohledem pro konfiguraci v budoucnosti. Dále pak srovnatelné skupiny musejí mít podobnou jmennou konvenci. Takto zajistíme nesporné určení uživatelů do předem připravených skupin.

Tab. 7. Příklady jmenných konvencí Globálního rozsahu (Global)

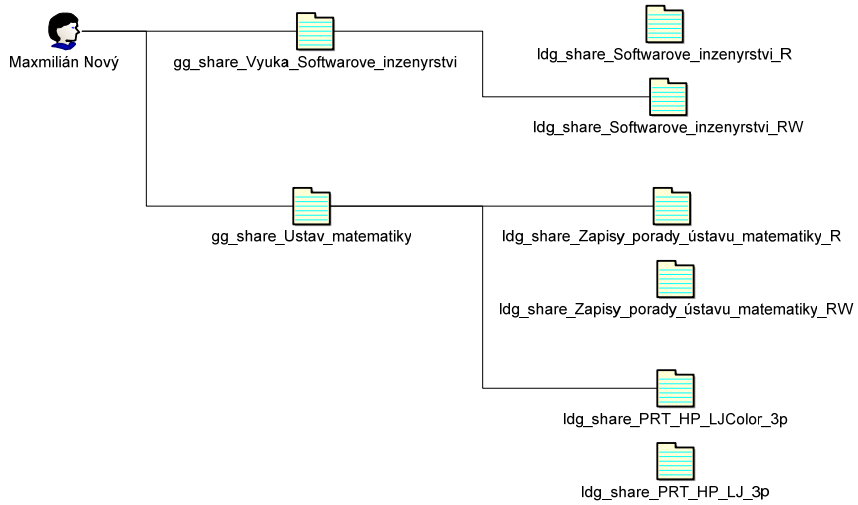
Globální rozsah (*Global*)	Popis
gg_share_Studenti	skupina obsahující účty studentů
gg_share_Vyuka_Softwarove_inzenyrstvi	skupina vyučujících - Softwarové inženýrství
gg_share_Ustav_matematiky	skupina zaměstnanců Ústavu matematiky
gg_share_Projekt_implementace_ADDS	projekt v rámci univerzity
gg_share_zamestnanci_3p	zaměstnanci – 3. Patro

Globální skupiny jsou po implentaci, nejvíce používané skupiny ze všech definovaných, protože do nich umísťujeme singulární uživatele.

Tab. 8. Příklady jmenných konvencí Místního lokálního rozsahu (Domain Local)

Místní lokální rozsah (Domain Local)	Popis
ldg_share_Vyuka_R	složka vyuka – oprávnění pro čtení
ldg_share_ Softwarove_inzenyrstvi_RW	složka SW_inzenyrstvi – oprávnění pro čtení / zápis
ldg_share_ Softwarove_inzenyrstvi_R	složka SW_inzenyrstvi – oprávnění pro čtení
ldg_share_PRT_HP_LJColor_3p	barevné tiskárny – 3. patro
ldg_share_PRT_HP_LJ_3p	černobílé tiskárny – 3. patro

Jak již bylo řečeno, *Místní lokální rozsah* je zacílen na zdroje skupin, které jsou přidělovány *Globálním rozsahům*. Pro lepší pochopení strategie *AGDLP* uvádím příklad použití.



Obr. 28. Příklad strategie Skupin

Uživatel Maxmilián Nový je členem *Globální skupiny gg_share_Vyuka_Softwarove_inzenyrstvi*, která mu umožňuje číst nebo psát do složky *Softwarove_inzenyrstvi*. Jako zaměstnanec Ústavu matematiky má oprávnění číst zápisy z porad svého ústavu a může tisknout na barevné tiskárny lokalizované ve třetím patře.

Při volbě *Typu skupin (Group Type)* je namístě určitá obezřetnost, protože pokud zvolíme velké množství skupin *Se zabezpečením (Security)* důsledkem je pravděpodobné snížení rychlosti systému, a proto je nezbytné vyhodnotit, ve kterých případech je vhodnější použít skupinu *Distribuční (Distribution)*.

Proces návrhu *Skupin* vyžaduje velmi detailní znalost organizační struktury, pracovních postupů a dalších drobných detailů. Bohužel, tímto typem informací disponují pouze zaměstnanci univerzity, proto komplexní řešení tohoto problému je na správci sítě a klíčových uživatelích.

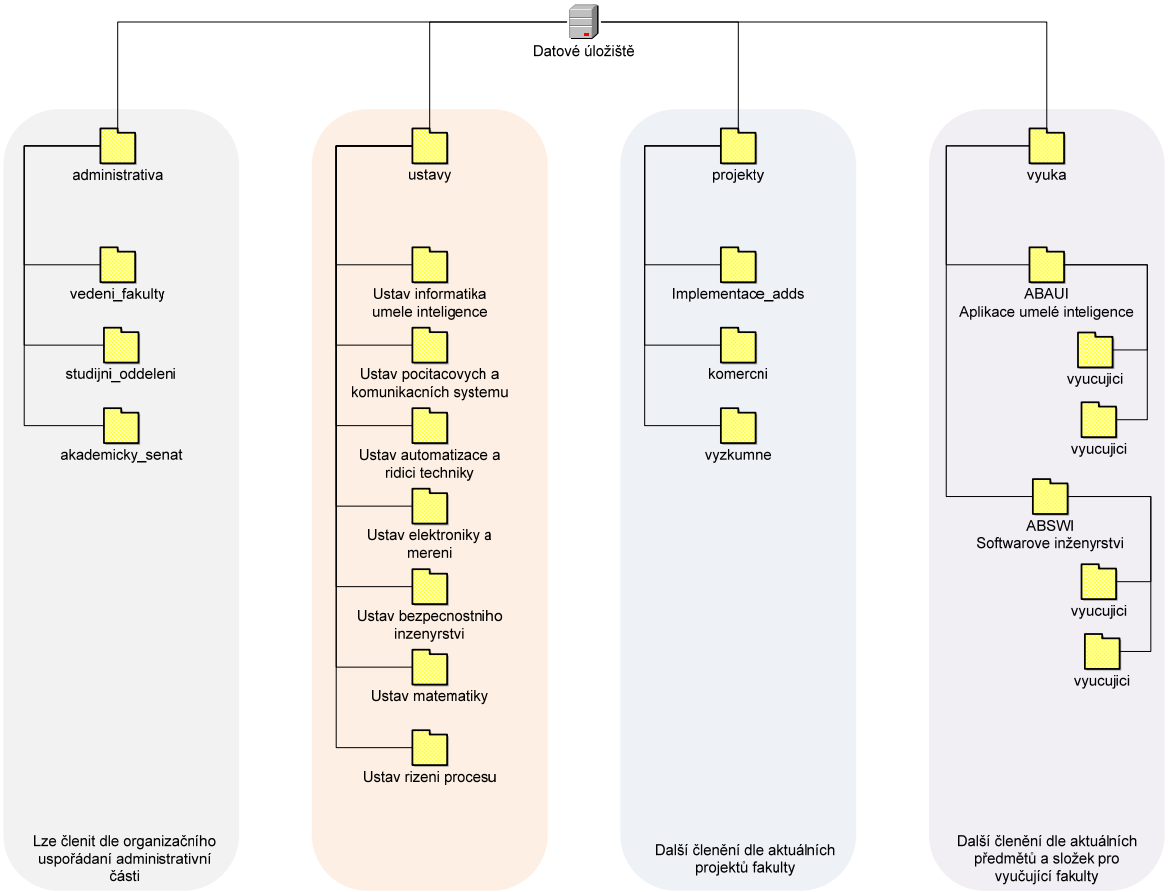
6.4 Adresářová sdílená struktura zdrojů skupin

Návrh sdílených složek publikovaných ve službě *Active Directory Domain Services* úzce souvisí s designem *Skupin*. Vycházíme-li z předpokladu 4 hlavních adresářů:

- administrativa,
- ustavy,
- projekty,

- vyuka,

pak další logickou stavbou sdílené adresářové struktury jsou složky, které nám organizačně nebo funkčně návrh zjemní a zpřehlední.



Obr. 29. Návrh adresářové struktury FAI

Stejně jako u projektování *Skupin*, je opět nezbytná detailní znalost prostředí připravovaného návrhu, proto je nutné tento nástin brát jako možnou cestu při stavbě nového adresářového prostředí.

6.5 Zásady skupin (Group Policy)

V této kapitole jsou definovány systémové politiky pro úroveň domény ***utb.local*** a *Organizačních jednotek (Organizational Unit)*. Zásady, které vynucené dědičnosti pro *OU* jsou vymezené v rovině domény.

Vzhledem ke skutečnosti, že systém *Windows Server 2008 R2* obsahuje významné množství nastavení systémových politik nejen pro *pracovní stanice (Computer Configuration),* ale i *uživatele (User Configuration)*, autor této práce nemůže mít komplexní znalosti požadavků na provoz a s ním spojenou bezpečnost počítačové sítě UTB ve Zlíně. Proto je nezbytné chápat následující souhrn *zásad* jako seznam doporučených nastavení. Při implementaci *Zásad skupin* je nanejvýš rozumné začínat u jednoduchých politik, na které bude postupem času aplikován režim zpřísnění a upřesnění.

6.5.1 Konfigurace počítače (Computer Configuration)

6.5.1.1 Zásady hesla

Tab. 9. Group Policy - Zásady hesla

Název	Nastavení
Heslo musí splňovat požadavky na složitost *(Password must meet complexity requirements)*	Enabled
Maximální stáří hesla *(Maximum password age)*	120 days
Minimální stáří hesla *(Minimum password age)*	5 days
Minimální délka hesla *(Minimum password length)*	10 characters
Ukládat hesla pomocí reverzibilního šifrování *(Store passwords using reversible encryption)*	Disabled
Vynutit použití historie hesel *(Enforce password history)*	5 passwords remembered

6.5.1.2 Zásady uzamčení účtů

Tab. 10. Group Policy - Zásady uzamčení účtů

Název	Nastavení
Doba uzamčení účtu *(Account lockout duration)*	30 minutes
Prahová hodnota pro uzamčení účtu *(Account lockout threshold)*	5 invalid logon attempts

Název	Nastavení
Vynulovat čítač uzamčení účtu po *(Reset account lockout counter after)*	30 minutes

6.5.1.3 Zásady auditu

Tab. 11. Group Policy - Zásady auditu

Název	Nastavení
Auditovat správu účtů *(Audit account management)*	Success, Failure
Auditovat systémové události *(Audit system events)*	Success, Failure
Auditovat události přihlášení *(Audit logon events)*	Success, Failure
Auditovat změny zásad *(Audit policy change)*	Success, Failure

6.5.1.4 Přiřazení uživatelských práv

Tab. 12. Group Policy - Přiřazení uživatelských práv

Název	Nastavení
Odepřít místní přihlášení *(Deny log on locally)*	gg_share_studenti
Povolit přihlášení prostřednictvím Vzdálené plochy *(Allow log on through Terminal Services)*	gg_share_IT_ADMIN
Zakázat přihlášení prostřednictvím Vzdálené plochy *(Deny log on through Terminal Services)*	gg_share_studenti

6.5.1.5 Možnosti zabezpečení

Tab. 13. Group Policy - Možnosti zabezpečení

Název	Nastavení
Interaktivní přihlašování: Nevyžadovat stisknutí kláves Ctrl+Alt+Del *(Interactive logon: Do not require CTRL+ALT+DEL)*	Disabled
Interaktivní přihlašování: Nezobrazovat naposledy použité uživatelské jméno *(Interactive logon: Do not display last user name)*	Enabled
Interaktivní přihlašování: Text zprávy pro uživatele pokoušející se přihlásit *(Interactive logon: Message text for users attempting to log on)*	Text pro uživatele
Interaktivní přihlašování: Vyzvat uživatele ke změně hesla před jeho	14 days

Název	Nastavení
vypršením *(Interactive logon: Prompt user to change password before expiration)*	
Účty: Přejmenovat účet správce *(Accounts: Rename administrator account)*	"novakova_eva"
Vypnutí: Umožnit vypnutí systému bez přihlášení *(Shutdown: Allow system to be shut down without having to log on)*	Enabled
Zařízení: Zabránit uživatelům instalovat ovladače tiskáren při připojení ke sdíleným tiskárnám *(Devices: Prevent users from installing printer drivers)*	Enabled

6.5.1.6 Protokol událostí

Tab. 14. Group Policy - Protokol událostí

Název	Nastavení
Maximální velikost aplikačního protokolu *(Maximum application log size)*	5440 kilobytes
Maximální velikost protokolu zabezpečení (Maximum security log size)	5440 kilobytes
Maximální velikost systémového protokolu *(Maximum system log size)*	5440 kilobytes
Metoda uchování aplikačního protokolu *(Retention method for application log)*	As needed
Metoda uchování protokolu zabezpečení *(Retention method for security log)*	As needed
Metoda uchování systémového protokolu *(Retention method for system log)*	As needed
Zabránit místní skupině Guests k aplikačnímu protokolu *(Prevent local guests group from accessing application log)*	Enabled
Zabránit místní skupině Guests k protokolu zabezpečení *(Prevent local guests group from accessing security log)*	Enabled
Zabránit místní skupině Guests k systémovému protokolu *(Prevent local guests group from accessing system log)*	Enabled

6.5.1.7 Brána Windows Firewall

Tab. 15. Group Policy - Brána Windows Firewall

Název	Nastavení
Brána Windows Firewall: Chránit všechna síťová připojení *(Windows Firewall: Protect all network connections)*	Enabled
Brána Windows Firewall: Povolit výjimku pro sdílení souborů a tiskáren pro příchozí spojení *(Windows Firewall: Allow inbound file and printer sharing exception)*	10.1.0.0/24
Brána Windows Firewall: Povolit výjimku protokolu ICMP *(Windows Firewall: Allow ICMP exceptions)*	Enabled
Brána Windows Firewall: Povolit výjimky místních programů *(Windows Firewall: Allow local port exceptions)*	Enabled
Brána Windows Firewall: Zakázat upozorňování *(Windows Firewall: Prohibit notifications)*	Enabled

6.5.1.8 Instalační služba systému Windows

Tab. 16. Group Policy - Instalační služba systému Windows

Název	Nastavení
Povolit uživatelům ovládat instalace *(Enable user control over installs)*	Disabled
Protokolování *(Logging)*	Enabled
Umožnit správci instalaci z relace služby Vzdálená plocha *(Allow admin to install from Remote Desktop Services session)*	Enabled

6.5.1.9 Internet Explorer

Tab. 17. Group Policy - Internet Explorer

Název	Nastavení
Zóny zabezpečení: Nepovolit uživatelům měnit zásady *(Security Zones: Do not allow users to change policies)*	Enabled
Zóny zabezpečení: Nepovolit uživatelům přidávat či odebírat servery *(Security Zones: Do not allow users to add/delete sites)*	Enabled
Neumožnit uživatelům povolovat či zakazovat doplňky *(Do not allow users to enable or disable add-ons)*	Enabled

Název	Nastavení
Zakázat zobrazení úvodní obrazovky *(Disable showing the splash screen)*	Enabled

6.5.1.10 Služba Vzdálená plocha

Tab. 18. Group Policy - Služba Vzdálená plocha

Název	Nastavení
Nastavit časový limit aktivních, ale nečinných relací služby Vzdálená plocha *(Set time limit for active but idle Remote Desktop Services sessions)*	15 minutes
Nepovolit přesměrování tiskárny klienta *(Do not allow client printer redirection)*	Enabled
Nepovolit přesměrování jednotek *(Do not allow drive redirection)*	Enabled
Umožňuje nastavit pravidla vzdáleného řízení uživatelských relací služby Vzdálená plocha. *(Set rules for remote control of Remote Desktop Services user sessions)*	Enabled

6.5.1.11 Zásady automatického přehrávání

Tab. 19. Group Policy - Zásady automatického přehrávání

Název	Nastavení
Vypnout automatické přehrávání (Turn off Autoplay)	Enabled

6.5.1.12 Zásady skupin

Tab. 20. Group Policy - Zásady skupin

Název	Nastavení
Interval aktualizace zásad skupiny pro počítače *(Group Policy refresh interval for computers)*	Enabled
Rozpoznání pomalého připojení zásad skupiny *(Group Policy slow link detection)*	Enabled

6.5.1.13 Tiskárny

Tab. 21. Group Policy - Tiskárny

Název	Nastavení
Interval aktualizace zásad skupiny pro počítače *(Group Policy refresh interval for computers)*	Enabled
Rozpoznání pomalého připojení zásad skupiny *(Group Policy slow link detection)*	Enabled

6.5.2 Konfigurace uživatele (User Configuration)

6.5.2.1 Nabídka Start a Hlavní panel

Tab. 22. Group Policy - Nabídka Start a Hlavní panel

Název	Nastavení
Nepovolovat připojování programů na hlavní panel *(Do not allow pinning programs to the Taskbar)*	Enabled
Nezobrazovat žádné vlastní panely nástrojů na hlavním panelu *(Do not display any custom toolbars in the taskbar)*	Enabled
Odebrat ikonu Síť z nabídky Start *(Remove Network icon from Start Menu)*	Enabled
Odebrat možnost přetahování myší a místní nabídky v nabídce Start *(Remove drag-and-drop and context menus on the Start Menu)*	Enabled
Odebrat odkaz Hledat počítač *(Remove Search Computer link)*	Enabled
Odebrat příkaz Hry z nabídky Start *(Remove Games link from Start Menu)*	Enabled
Odebrat síťová připojení z nabídky Start *(Remove Network Connections from Start Menu)*	Enabled
Uzamknout hlavní panel *(Lock the Taskbar)*	Enabled
Uzamknout všechna nastavení hlavního panelu *(Lock all taskbar settings)*	Enabled
Zabránit změnám nastavení hlavního panelu a nabídky Start *(Prevent changes to Taskbar and Start Menu Settings)*	Enabled

6.5.2.2 Ovládací panely

Tab. 23. Group Policy - Ovládací panely

Název	Nastavení
Zakázat přístup k Ovládacím panelům *(Prohibit access to the Control Panel)*	Enabled
Zobrazit pouze určené panely v Ovládacích panelech *(Show only specified Control Panel items)*	Enabled
Časový limit spořiče obrazovky *(Screen saver timeout)*	Seconds: 300
Chránit spořič obrazovky heslem *(Password protect the screen saver)*	Enabled
Povolit spořič obrazovky *(Enable screen saver)*	Enabled
Zabránit změnám pozadí plochy *(Prevent changing desktop background)*	Enabled
Zabránit odstraňování tiskáren *(Prevent deletion of printers)*	Enabled
Skrýt kartu Nastavení *(Hide Settings tab)*	Enabled

6.5.2.3 Přidat nebo ubrat programy

Tab. 24. Group Policy - Přidat nebo ubrat programy

Název	Nastavení
Odebrat položku Přidat nebo odebrat programy *(Remove Add or Remove Programs)*	Enabled
Skrýt možnost Přidat program z disku CD-ROM nebo z diskety *(Hide the "Add a program from CD-ROM or floppy disk" option)*	Enabled
Skrýt možnost Přidat programy získané od společnosti Microsoft *(Hide the "Add programs from Microsoft" option)*	Enabled
Skrýt možnost Přidat programy získané ze sítě *(Hide the "Add programs from your network" option)*	Enabled
Skrýt stránku Přidat nebo odebrat součásti systému Windows *(Hide Add/Remove Windows Components page)*	Enabled
Přejít přímo na Průvodce součástmi systému Windows *(Go directly to Components Wizard)*	Enabled
Odebrat informace o podpoře *(Remove Support Information)*	Enabled

6.5.2.4 Plocha

Tab. 25. Group Policy - Plocha

Název	Nastavení
Tapeta plochy *(Desktop Wallpaper)*	Enabled
Odebrat příkaz Vlastnosti z místní nabídky ikony Počítač *(Remove Properties from the Computer icon context menu)*	Enabled
Zakázat změny *(Prohibit changes)*	Enabled

6.5.2.5 Instalační služba systému Windows

Tab. 26. Group Policy - Instalační služba systému Windows

Název	Nastavení
Zakázat všechny instalace z vyměnitelných médií *(Prevent removable media source for any install)*	Enabled

6.5.2.6 Internet Explorer

Tab. 27. Group Policy - Internet Explorer

Název	Nastavení
Zakázat změnu nastavení domovské stránky *(Disable changing home page settings)*	Home Page www.utb.cz
Zakázat změnu nastavení certifikátů *(Disable changing certificate settings)*	Enabled
Zakázat změnu nastavení barev *(Disable changing color settings)*	Enabled
Zakázat změnu nastavení hodnocení *(Disable changing ratings settings)*	Enabled
Zakázat změnu nastavení stránky Rozšířené *(Disable changing Advanced page settings)*	Enabled
Zapnout automatické dokončování pro uživatelská jména a hesla ve formulářích *(Turn on the auto-complete feature for user names and passwords on forms)*	Disabled
Zakázat stránku Připojení *(Disable the Connections page)*	Enabled
Zakázat stránku Programy *(Disable the Programs page)*	Enabled
Zakázat stránku Rozšířené *(Disable the Advanced page)*	Enabled
Zakázat stránku Zabezpečení *(Disable the Security page)*	Enabled

6.5.2.7 *Konzola Microsoft Management Console*

Tab. 28. Group Policy - Konzola Microsoft Management Console

Název	Nastavení
Omezit přístup uživatelů pouze k výslovně povoleným modulům snap-in *(Restrict users to the explicitly permitted list of snap-ins)*	Enabled
Zabránit uživateli přejít do autorského režimu *(Restrict the user from entering author mode)*	Enabled

6.5.2.8 *Průzkumník Windows*

Tab. 29. Group Policy - Průzkumník Windows

Název	Nastavení
Odebrat kartu Hardware *(Remove Hardware tab)*	Enabled
Odebrat kartu Zabezpečení *(Remove Security tab)*	Enabled
Odebrat možnost měnit nastavení animace nabídek pomocí uživatelského rozhraní *(Remove UI to change menu animation setting)*	Enabled
Odebrat příkazy Připojit síťovou jednotku a Odpojit síťovou jednotku *(Remove "Map Network Drive" and "Disconnect Network Drive")*	Enabled
Zakázat ikonu Celá síť ve složce Místa v síti *(No Entire Network in Network Locations)*	Enabled
Zakázat položku Okolní počítače ve složce Umístění v síti *(No Computers Near Me in Network Locations)*	Enabled

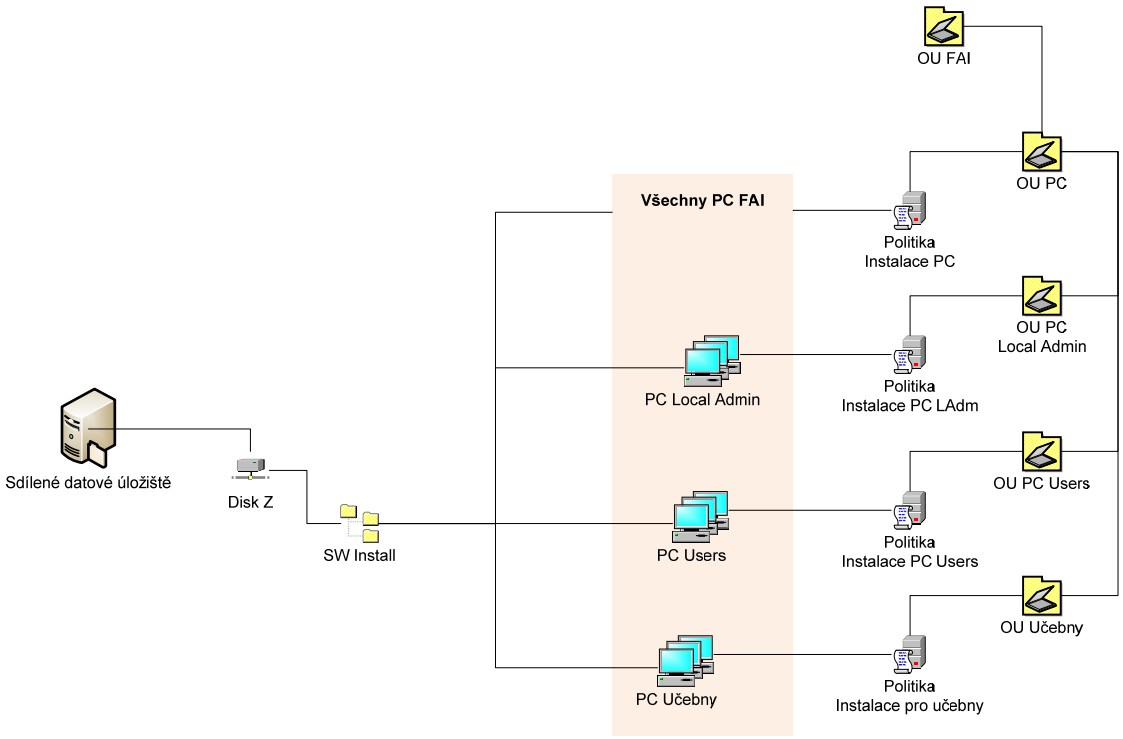
6.5.3 Instalace aplikací

Instalace software pomocí *Zásad skupin (GPO)* můžeme zacílit buď na *počítače (Computers)* nebo *uživatele (Users)*, proto je potřeba vnímat dopady na tyto skupiny. Pokud budeme instalovat aplikace na skupinu:

- *Computers*, bude mít každý uživatel, pracující na daném počítači, možnost využívat nainstalované aplikace, ve srovnání s
- *Users*, pokud bude využívat neustále jiné počítače, budou se jeho přidělené aplikace s každou touto změnou instalovat.

V rámci *GPO* lze na jednotlivé uživatele aplikovat restrikce, které zpřísní používání software.

V rámci návrhu budou instalace zaměřené na *počítače (Computers)* umístěné v singulárních *Organizačních jednotkách (Organizational Unit)* dodržující pravidlo nejvyššího umístění při instalacích stejného software pro více pracovních stanic.



Obr. 30. Group Policy – Instalace aplikaci FAI

Instalaci aplikací je nevyhnutné rozdělit do následujících kroků:

- příprava instalačního balíčku Windows (*.wmi) nebo pro starší aplikace *.zap,
- rozhodnutí zda Publikovat nebo Zveřejňovat,
- určení pro jakou skupinu má být instalace aplikována,
- vytvoření sdíleného úložiště pro uložení instalačních souborů a s ním spojené oprávnění sdílení,
- vytvoření *zásady skupin* (*GPO*) pro nasazení software,
- testování instalace.

Při aplikaci je dobré vnímat skutečnost, že aktualizací aplikací od společnosti Microsoft, řeší služba *Windows Server Update Services* a její nastavení v *Zásadách skupin*. Aplikace balíčků *Servis Pack* může mít různé cesty, které budou závislé na přístupu administrátorů UTB ve Zlíně.

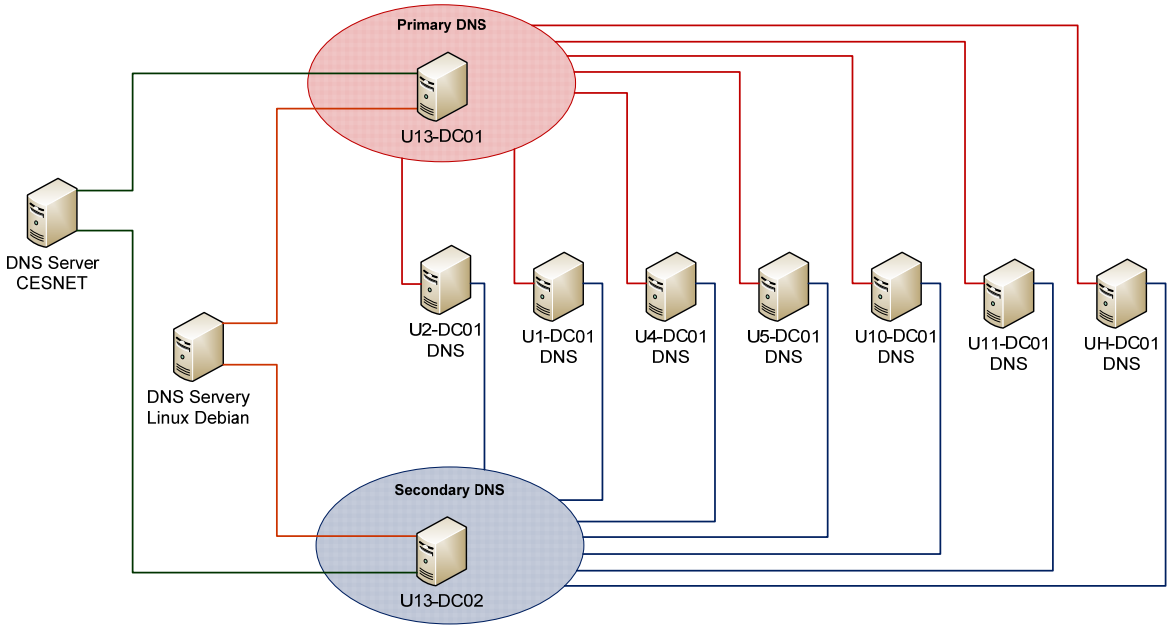
6.5.4 Delegování oprávnění na GPO (Delegation)

Předání a rozložení pravomocí vyžaduje delegování oprávnění na objekty *GPO*. Řízení delegování na úrovni *OU* bude probíhat takto:

- hlavní správce vynucuje, spravuje politiky a ošetřuje nastavení na úrovni domény,
- pověření správci zajišťují správu na jednotlivých fakultách s tím, že nemohou změnit vynucené dědičnosti z úrovně domény,
- studijní oddělení vytváří, odstraňuje a spravuje uživatelské účty uživatele na úrovni Studenti,
- personální oddělení vytváří, odstraňuje a spravuje uživatelské účty uživatele na úrovni Zaměstnanci.

7 ROLE DOMAIN NAME SYSTEM

Návrh DNS (***D**omain **N**ame **S**ystem*) je založen na schématu se samostatnými názvy a je postavený na záměrném oddělení interní sítě (doména ***utb.local***) a veřejné prezentace v Internetu (doména ***utb.cz***). Tento model je v zásadě jednodušší ve smyslu konfigurace a předchází některým vnitropodnikovým komunikačním šumům při vytváření veřejných subdomén, které při aplikaci schématu *split-brain* (interní i externí domény stejné) nutně potřebují vytvořit dodatečné záznamy v nastavení. Název domény *utb.local* nemusíme registrovat, protože *.local* není veřejná doména nejvyšší úrovně.



Obr. 31. DNS servery pro doménu utb.local

7.1 Servery

Návrh DNS servery pro doménu utb.local:

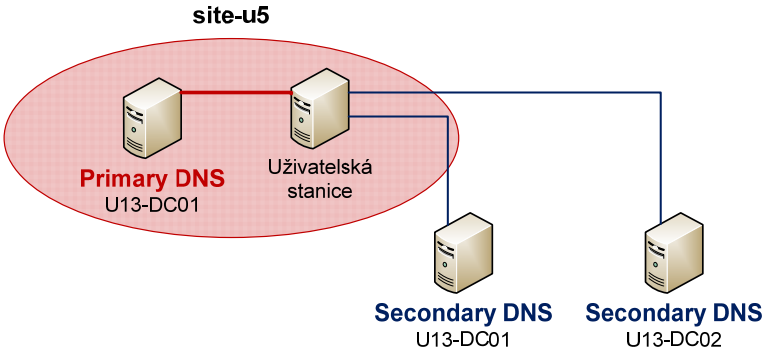
- DNS servery budou součástí *Doménových řadičů (Domain controller)* domény *utb.local*,
- DNS zóny budou integrovány v *Active Directory*,
- *Servery pro předání (Forwarders)* budou nastaveny na U13-DC01 a U13-DC02,

- překlad externích jmen pro klienty domény bude řešen předáváním dotazu na externí DNS server (DNS Servery Linux Debian a DNS Server CESNET),
- budou povoleny jen zabezpečené aktualizace (*Allow Only Secure Dynamic Updates*),
- každý interní *DNS Server* bude nastaven tak, aby ve své IP konfiguraci se odkazoval sám na sebe.

7.2 Klientské stanice

Konfigurace DNS klientů pro doménu utb.local:

- klientské stanice by měly mít nakonfigurovány minimálně dva *DNS Servery*,
- primární *DNS Server* bude vždy takový server, který je jako *DC* v *Lokalitě (Site)*, jejíž součástí je i klientský počítač,
- sekundární *DNS Servery* budou U13-DC01 a U13-DC02.



Obr. 32. Konfigurace DNS klientů pro FAI

8 METODIKA ADMINISTRACE A BEZPEČNOST

Jednou z klíčových kapitol při implementaci jakéhokoliv systému je metodika administrace a aplikace bezpečnosti, jak před útokem z externí, tak i interní části sítě.

Zabezpečení je proces vyžadující strategické uvažování. V první fázi pojmenuje hrozící rizika informacím a následně určí, jaká rizika jsou přijatelná. Ve druhé fázi stanoví technické řešení, nezbytné pro jeho snížení, protože riziku se nelze vyhnout.

Základní bezpečnostní administrace v prostředí *Windows Server 2008 R2* je prováděna nativními nástroji *Microsoft Management Console (Active Directory Users and Computers, Active Directory Site and Services aj.).*

8.1 Pravomoci v systému

Rozdělení pravomocí v administrativním prostředí je přímo závislé na specializaci, zkušenosti a odpovědnosti daného pracovníka. Jednou z cest je vytvoření týmu administrátorů, kteří budou mít dostatečná práva v systému (dle specializace) a kteří budou přímo odpovědni za funkčnost celého systému.

Administrátoři jsou rozčleněni do místních, místních doménových a globálních předdefinovaných skupin *(Security groups)* dle svého zaměření:

- *Administrators,*
- *Domain Admins,*
- *Account Operators* aj.

Pro větší stupeň zabezpečení, bude účet *Administrátor* zablokován a pro účely administrace v těchto důležitých skupinách bude založen nový účet, který bude splňovat nejvyšší požadavky na zabezpečení s použitím neutrálního názvu tohoto účtu (název nesmí ani okrajově připomínat svůj účel).

Účet Administrátor slouží pouze k administrativním úkonům a nikoliv k rutinnímu zpracování dat v systému!!!

8.2 Úrovně diskrétnosti

V rámci univerzity musí existovat přehledný návrh oddělující informace v rámci diskrétnosti definující jejich stupeň:

- přísně soukromé,
- soukromé,
- veřejné – studenti,
- veřejné.

Zvolená úroveň diskrétnosti musí zabezpečovat snížení rizik, odhalení citlivých dat (úmyslně nebo omylem) a dostupnost informací v rámci zvolených bezpečnostních skupin.

Důvěrnost lze v systému *Windows Server 2008 R2* lze zabezpečit nativními nástroji např:

- služba správy přístupových práv,
- služba IPSec,
- virtuální privátní sítě,
- systém souborů EFS.

8.3 Pravidla zabezpečení

Při tvorbě pravidel zabezpečení bude nevyhnutelné zajistit odpovědi na otázky typu:

- Jaké potřebuje uživatel minimální práva pro svou činnost?
- Jaký je nejslabší článek zabezpečení na naší síti?
- Jaký bude důsledek, když odejde klíčový zaměstnanec nebo administrátor?
- Znají uživatelé bezpečnostní rizika spojená s jejich chováním na síti?
- Zabezpečíme pravidelné testování na zranitelná místa v síti?
- Je vytvořen systém odpovědnosti na síti?

Na první pohled neobsahuje tento malý seznam plný výčet otázek, podle kterých se připravují pravidla zabezpečení, ovšem v případě podcenění tvorby těchto pravidel nám určitě budoucnost připraví často neřešitelné situace a také samozřejmě zvyšujeme míru neakceptovatelných rizik.

Pravidla vládnou bezpečnosti a uživatelé s účtem *Administrátor* je v **žádném případě nesmí porušovat**, bohužel, praxe nám často ukazuje opak. Výjimky, jak dočasné nebo trvalé, mívají fatální následky.

8.4 Bezpečnostní skupiny uživatelů

Základní rozdělení bezpečnostních skupin uživatelů:

- administrátoři,
- zaměstnanci,
- studenti.

Další rozdělení je závislé na zdroji úrovní citlivých informací a jejich publikování jak veřejném, tak interním.

8.5 Zabezpečení účtů

Jak již bylo řečeno v kapitole Pravomoci v systému, bude výchozí účet *Administrátor* zakázán a nevyhnutelné je *splnění požadavků na složitost (Password Must Meet Complexity Requirements)*.

Vlastnosti hesla:

- musí obsahovat malá písmena (a-z), velká písmena (A-Z), číslice (0-9) a znaky (@&#$%?!),
- nesmí mít logickou strukturu (obsahovat slovo),
- nesmí obsahovat uživatelské jméno,
- složitost hesla musí být nejméně 8 znaků
    - studenti 8 znaků,
    - zaměstnanci 10 znaků a více,
    - administrátoři 20 a více znaků.

Pro účty *Administrátor* je doporučené dvojúrovňové ověřování = použití dvou metod k jednoznačnému ověření uživatele, například přidání čtečky biometrických údajů.

8.6 Školení uživatelů

Pravidelné školení uživatelů, při kterém se zdůrazní bezpečnostní rizika a nutnost používání komplexních a dlouhých hesel, přispěje k samozřejmému bezpečnému využívání systému.

Osvědčenými systémy školení jsou modelové situace a scénáře, které jsou blízké pracovnímu prostředí, ve kterém se uživatel nachází.

8.7 Směrnice - Pravidla užívání počítačové sítě

Zveřejněná pravidla, která jasně definují užívání počítačové sítě, počítačů, tiskáren a jiných zařízení mající vztah k IT.

Směrnice by měla zahrnovat:

- základní pojmy – co je počítačová stanice, HW, SW, počítačová síť, administrátor sítě, uživatel apod.,
- služby poskytované univerzitou uživatelům sítě,
- ochrana dat a informací,
- přístupová práva a identifikace uživatele,
- práva a povinnosti uživatele,
- práva a povinnosti administrátora sítě,
- monitorování,
- postihy za nedodržení pravidel.

Jasná a srozumitelná definice jednotlivých bodů svým dílem přispívá k bezproblémovému chodu celého systému.

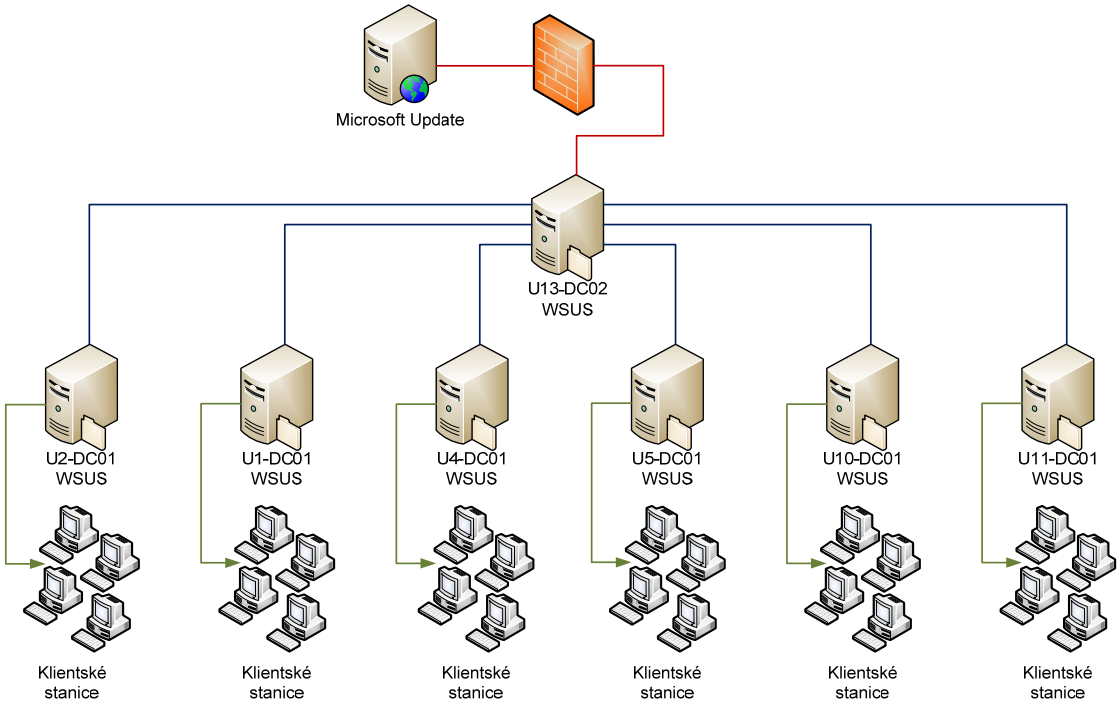
9 NETWORK TIME PROTOCOL

Pro správnou činnost primárního autentizačního protokolu *Kerberos V5* je důležitá - nezbytná synchronizace systémového času na všech zařízeních připojených do sítě - nejen počítačových stanic, ale i serverů. Bezchybný chod replikací *Active Directory Domain Services* a *Domain Name System* je zabezpečený synchronizací systémového času *Doménových řadičů (Domain Controller)* a rozhodujícím činitelem při konfliktu je *Time Stamp*.

- Základní *TimeEtalon Server*: **U13-DC01**,
- synchronizace s: **ntp.utb.cz**.

10 WINDOWS SERVER UPDATE SERVICES

Efektní a rychlý způsob aktualizace - udržování aktuálnosti systémů - pro opravy a aktualizace nabízí služba *Windows Server Update Services (WSUS)*.



Obr. 33. Návrh Windows Server Update Services pro UTB ve Zlíně

Nastavení:

- opravy a aktualizace bude centrálně stahovat, přímo z *Microsoft Update*, server U13-DC02,
- pro ostatní doménové řadiče s instalovaným WSUS bude server U13-DC02 nastaven jako nadřazený,
- na WSUS serveru U13-DC02 bude odpovědný správce povolovat opravy a aktualizace pro produkty společnosti Microsoft,
- v *GPO (Group Policy)* budou nastavené politiky, které upřesní, jakým způsobem se aplikují povolené opravy a aktualizace na stanice a servery,
- hlavní a místí správci sítí budou pravidelně dostávat e-mailem hlášení o nových aktualizacích.

11 ZÁLOHA A OBNOVA

Ve své podstatě základní metodou zálohování *Active Directory Domain Services* je replikace na další *Řadiče domény (Domain Controllers),* v našem případě 9 *DC*. Navzdory tomu musí být *DC* zálohován. Při zálohování musí být pohlídána životnost objektu, tento fakt klade vysoké nároky na frekvenci zálohování.

Tato kapitola se nebude zabývat pravidelnou zálohou dat, která je postavena na denní či hodinové četnosti, ale jejím cílem je **ZDŮRAZNIT NALÉHAVOST ULOŽENÍ SOUČASNÉHO NASTAVENÍ PŘED JAKÝMKOLIV ZÁSAHEM DO SYSTÉMU** *Windows Server 2008 R2*.

Pro zálohu a obnovu dat budeme využívat nativních služeb systému (Windows Server Backup, LDP.exe, NTDSUtil aj.).

12 INSTALACE, KONFIGURACE A TESTY

Instalace a konfigurace probíhala v rámci testů na virtuálních serverech, které zaručují plnou funkčnost jak serverových systémů *Windows Server 2008 R2*, tak grafických operačních systémů určených až na výjimky pro počítačové stanice řady Windows XP a Windows 7.

12.1 Instalace a konfigurace

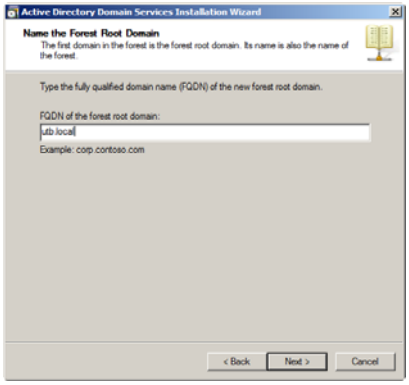
Záměrem této kapitoly není vytvoření „Step by Step" manuálu, ale jen nástin instalace *Active Directory Domain Services* a s ní spojené zavedení domény ***utb.local***, vytvoření *Doménových řadičů (Domain controllers)*, *Lokalit (Sites)* a *DNS Serverů*.

Celá instalace vychází z popsaného návrhu *AD DS*, která je charakterizována výše a jasně definuje server, který je určen jako jediný autoritativní server - *hlavní operační server* (*Operations Master*) a samozřejmě plní roli *FSMO*. Tento server bude instalován jako první a vzhledem k zavedení jmenných konvencí se bude nazývat **U13-DC01**.

12.1.1 Active Directory Domain Services a Domain Name System

Instalace *Active Directory Domain Services* bude spuštěna pomocí příkazu ***dcpromo.exe*** z příkazové řádky. Zároveň budeme instalovat roly *DNS (Domain Name System)* a *Globální katalog (Global Catalog, GC)*:

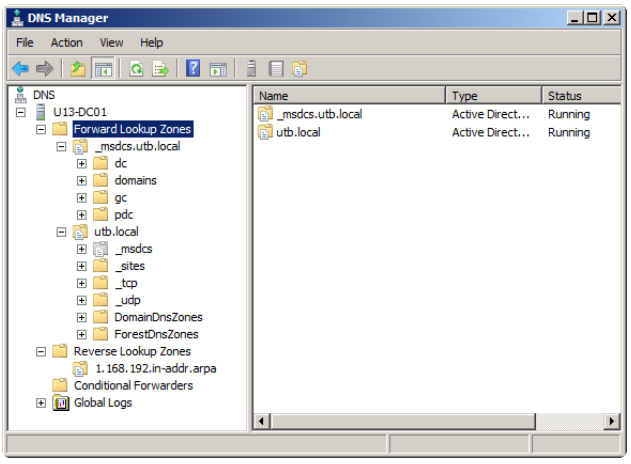
- potvrzením příkazu *dcpromo.exe* se rozeběhne průvodce instalací, který nás upozorní na kompatibilitu operačního systému,
- vytvoříme a pojmenujeme novou doménu ***utb.local***,
- po potvrzení instalace role *DNS* a *GC*,
- zvolíme bezpečné heslo pro Administrátora domény a
- po vytvoření komplexní struktury nám oznámí průvodce úspěšné dokončení úlohy.



Obr. 34. Název domény

Dále budeme pokračovat nastavením role DNS a to tak:

- *Servery pro předání (Forwarders)* budou nastaveny na DNS Servery Linux Debian a DNS Server CESNET,
- povolené jen zabezpečené aktualizace (*Allow Only Secure Dynamic Updates*),
- interní DNS Server bude nastaven tak, aby se ve své IP konfiguraci odkazoval sám na sebe.



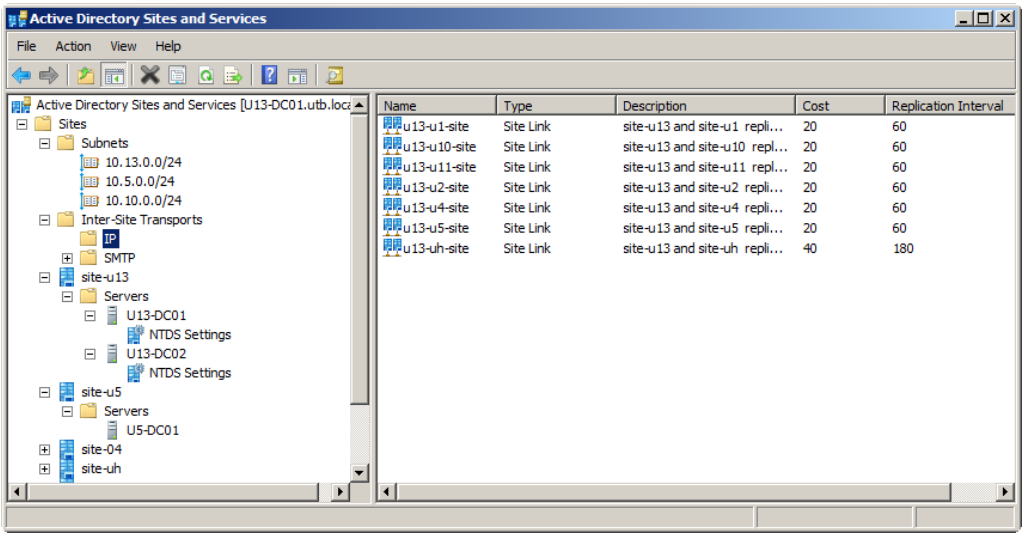
Obr. 35. Role DNS

Stejným způsobem se budou instalovat i ostatní *DC* s tím rozdílem, že se nebude vytvářet nová doména, ale využijeme volbu v *Přidat řadič domény do již existující domény (Add a domain controller to an existing domain)*.

12.1.2 Lokality (Site)

V modulu *Lokality a služby Active Directory (Active Directory Sites and Services)* se budou konfigurovat:

- jednotlivé *Lokality (Site)*,
- do *Lokalit* se umístí *Doménové řadiče (Domain Controllers)*,
- vytvoříme *Subnety (Subnets)* a
- replikace mezi *Lokalitami*.



Obr. 36. Konfigurace Lokalit (Sites)

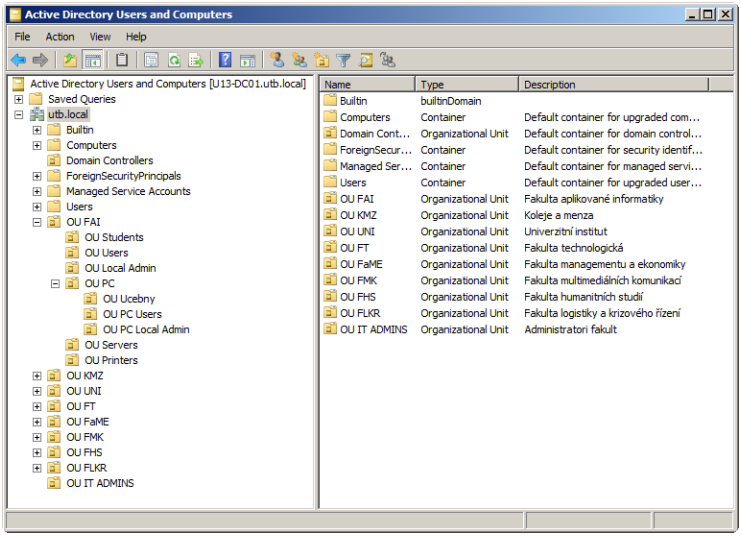
K testování replikačního propojení mezi servery se používá příkaz ***repadmin*** a pro kontrolu chyb replikace mezi *Řadiči domény* se aplikuje ***dcdiag***.

12.1.3 Organizační jednotky (Organizational Units)

Modul *Uživatelé a počítače služby Active Directory (Active Directory Users and Computers)* nám umožní nejen vytvářet a popisovat *Organizační jednotky* domény ***utb.local***, ale i umísťovat do těchto jednotek, uživatele, skupiny, sdílené tiskárny, počítače a další prvky *AD DS*.

Při zavádění *OU* je také možné použít řádkový příkaz:

dsadd ou "ou=FAI, dc=utb, dc=local" -desc "popis_ou " –d utb.local –u Administrator –p Pa$$w0rd

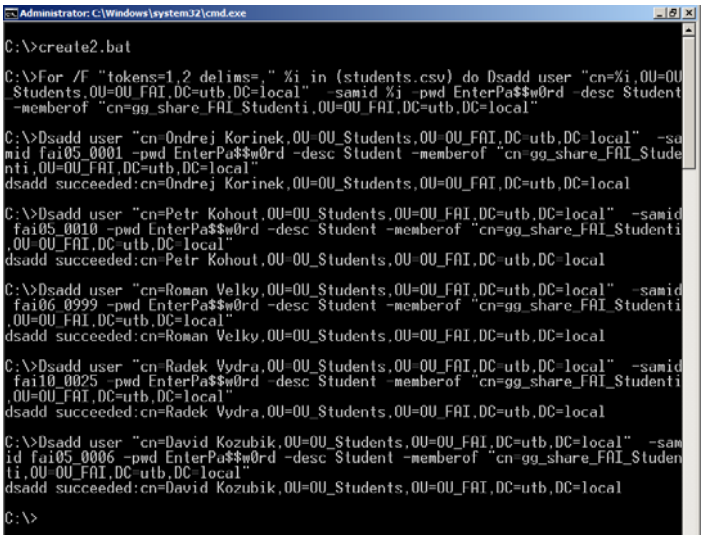


Obr. 37. Organizační jednotky (Organizational Unit)

12.1.4 Uživatelé, počítače a skupiny

Ve stejném grafickém modulu *Uživatelé a počítače služby Active Directory* se zavádějí uživatelé, počítače a skupiny. V prostředí Univerzity Tomáše Bati ve Zlíně bude minimálně jednou ročně nutné vytvořit nebo smazat velké množství uživatelských účtů. Běžně se k těmto úkonům používají skripty nebo nativní řádkové příkazy spojené s databází uživatelů, kteří byli použiti v následujícím příkladu.

For /f "tokens=1,2 delims=," %%i in (students.csv) do Dsadd user "cn=%%i,OU=OU_Students,OU=OU_FAI,DC=utb,DC=local" -samid %%j -pwd EnterPa$$w0rd -desc Student -memberof "cn=gg_share_FAI_Studenti,OU=OU_FAI,DC=utb,DC=local"



Obr. 38. Hromadné doplnění uživatelů

12.2 Testování scénářů Zásad skupin

Pro testování *Zásad skupin (GPO)* bylo vybráno několik variant scénářů pro uživatele a skupiny typu:

1. Student,
2. Zaměstnanec (vyučující),
3. Zaměstnanec studijního oddělení a
4. Local Admin.

Všechna použitá jména jsou pouze fiktivní, jakákoliv shoda je čistě náhodná. Scénáře budou simulovat restrikce, vzdálené instalace, mapování disků, delegování práv pro definované *Organizační jednotky (OU)* a jiné další v praxi předpokládané nastavení při použití nativních služeb *Windows Server 2008 R2*. Detailní konfigurace všech použitých zásad jsou v PŘÍLOZE PIII.

Vyjdeme z předpokladu, že do skupiny základních uživatelů, na které budeme aplikovat nezbytné restrikce, patří jak skupina Studenti, tak skupina Zaměstnanci. Zvláštní privilegium k užívání koncových stanic mají Local Admins, kteří jsou odpovědní za své počítače.

12.2.1 Scénář – Doména

- vynucená nastavení pro celou doménu
  - nezobrazovat poslední použité Uživatelské jméno,
  - sdílené datového úložiště pro vzdálené instalace.

12.2.2 Scénář – Student

- jednotný vzhled pozadí na počítači,
- spořič obrazovky chráněný heslem,
- jednotná Home Page v Internet Exploreru,
- zákaz stahování souborů přes Internet Explorer,
- zákaz modifikace Ovládacích panelů,
- zákaz modifikace Editoru registrů,
- přístup k zveřejněným podkladům ke studiu,
- heslo musí splňovat podmínky složitosti s délkou 8 znaků.

12.2.3 Scénář – Zaměstnanec (vyučující)

- restrikce stejné jako skupina Studenti, ale
- heslo musí splňovat podmínky složitosti s délkou 10 znaků,
- možnost číst a editovat podklady ke studiu,
- přístup ke sdíleným adresářům fakulty.

12.2.4 Scénář – Zaměstnanec Studijního oddělení

- stejné nastavení jako běžní zaměstnanci,
- delegovaná práva nad skupinou Studenti.

12.2.5 Scénář – Local Admin

- jednotný vzhled pozadí na počítači,
- spořič obrazovky chráněný heslem,
- koncová stanice v plné režii daného uživatele.

12.2.6 Použití zásad

V první fázi musíme definovat společné politiky, které budou děděné pro celou doménu *utb.local*.

Tab. 30. Společné doménové zásady

Název Politiky	Popis	Cíl
c_not_display_logon_name_policy	Nebude zobrazováno poslední použité uživatelské jméno.	doména utb.local
u_diskF_install_policy	Mapování disku F – sdílené informace pro vzdálenou instalaci.	doména utb.local
Default Domain Policy	Definice základních zásad hesel a uzamčení účtů	doména utb.local

Dále vymezíme zásady, které jsou společné pro různé druhy uživatelských skupin umístěných do *Organizačních jednotek (OU)* v doméně *utb.local*.

Tab. 31. Společné zásady OU Students a OU Users

Název Politiky	Popis	Cíl
u_restrict_desktop_background_policy	Konfigurace jednotného pozadí	OU Students OU Users OU Local Admin
u_security_screen_saver_policy	Konfigurace jednotného spořiče obrazovky, chráněného heslem.	OU Students OU Users OU Local Admin
u_restrict_control_panel_policy	Restrikce Ovládacích panelů	OU Students OU Users
u_restrict_acces_registry_policy	Restrikce spuštění Editora registrů	OU Students OU Users
u_IE_home_page_policy	Nastavení Home Page a Oblíbených položek	OU Students OU Users
u_IE_allow_file_download_policy	Restrikce stahování souborů z Internetu	OU Students OU Users
u_diskV_vyuka_policy	Mapování disku V – podklady pro výuku	OU Students OU Users

Jako poslední definujeme singulární nastavení *OU* v doméně *utb.local*.

Tab. 32. Singulární zásady

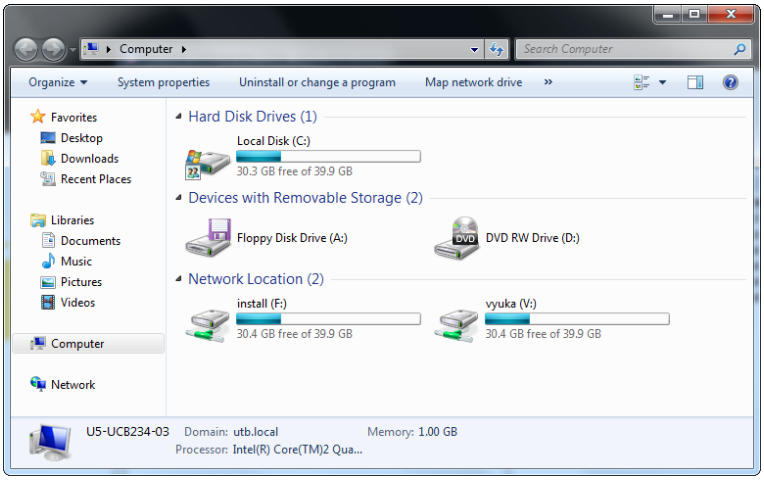
Název Politiky	Popis	Cíl
c_restrict_autoplay_CD_policy	Restrikce automatického spuštění CD	OU PC
c_remote_desktop_pc_policy	Povolení přístupu ke vzdálené ploše	OU PC
u_diskX_fai_policy	Mapování disku X – sdílené adresáře fakulty	OU Users

12.2.7 Testování uživatele - student

Testovaný uživatel: Student Tomáš Veselý

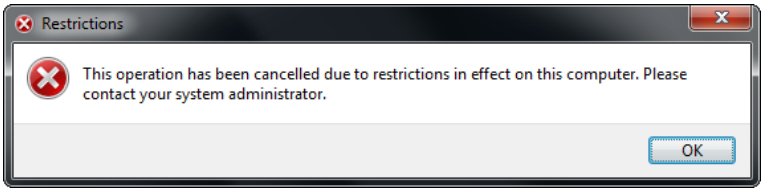
- přihlašovací jméno: fai09_0045
- členem skupin: gg_share_studenti

Po přihlášení se do domény má uživatel k dispozici dva sdílené disky, instalační disk ***F*** *(install)* a disk se zdroji k výuce ***V*** *(vyuka)*.



Obr. 39. Sdílené disky

Důsledkem restrikce na *Ovládací panely* je skutečnost, že *Start menu* neobsahuje odkaz na konfiguraci těchto panelů. Následné použití příkazu *control.exe* vyvolá chybové hlášení s informací o restrikci na tomto počítači a kontaktování Správce.



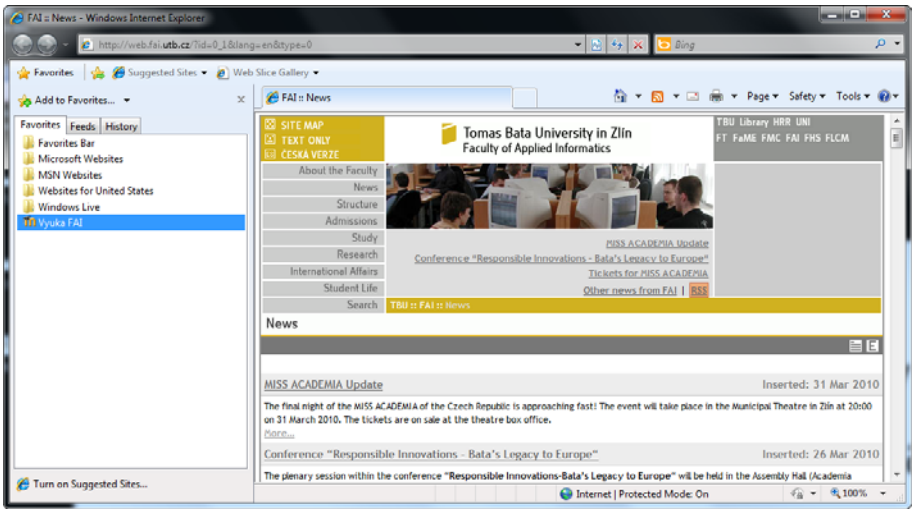
Obr. 40. Chybové hlášení – restrikce Ovládací panely

Při pokusu o konfiguraci *Editoru registrů* jsme upozorněni, že *„Registry editing has been disabled by your administrator“*.

Zásadou *u_restrict_desktop_background_policy* je aplikování jednotného počítačového pozadí spolu se spořičem obrazovky, který je chráněn heslem.

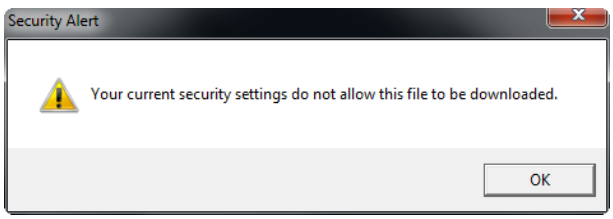
Obr. 41. Jednotné počítačové pozadí

Domovská stránka v prohlížeči *Internet Explorer* je nastavena na fakultní stránky a v *Oblíbených položkách* je odkaz na internetové stránky *Výuka FAI*.



Obr. 42. Nastaveni Internet Exploreru

Testovaný uživatel ***fai09_0045*** se při pokusu o stažení souboru z Internetu setká s chybovým hlášením, které ho upozorní na nemožnost tohoto úkonu.



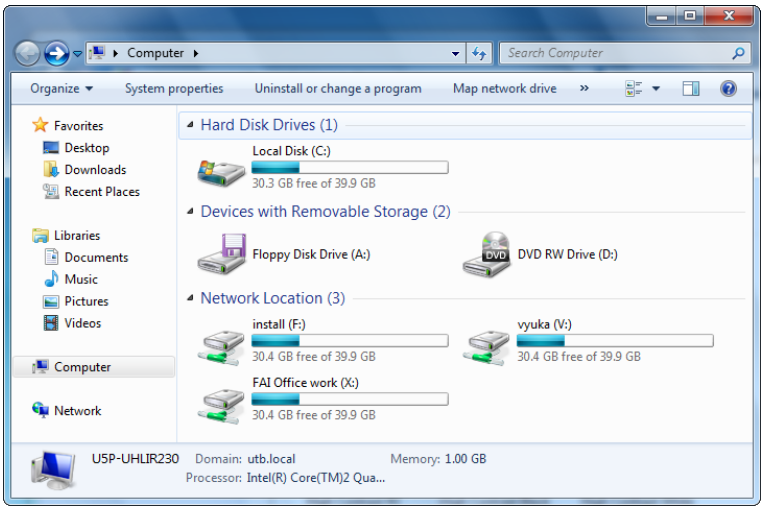
Obr. 43. Chybové hlášení IE

12.2.8 Testování uživatele - zaměstnanec

Testovaný uživatel: Zaměstnanec Petr Uhlíř

- přihlašovací jméno: uhlir_petr
- členem skupin: gg_share_zamestnanci_RW

Skutečnost, že společné restrikce a nastavení u Studentů a Zaměstnanců jsou totožné, byl výsledek testování stejný jako u předchozího uživatele. Rozdílné jsou pouze v aplikovaných právech disku ***V*** *(vyuka)* na čtení / zápis a přibyl nový disk ***X*** *(FAI Office work)* pro přístup k fakultním sdíleným složkám.



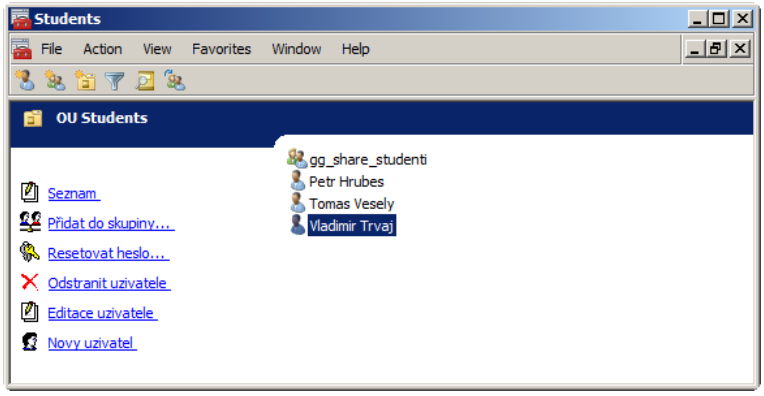
Obr. 44. Sdílené disky Zaměstnanci

12.2.9 Testování uživatele – Studijní oddělení

Testovaný uživatel: Markéta Dobrovolná

- přihlašovací jméno: dobrovolna_mark
- členem skupin: gg_share_zamestnanci_RW, gg_share_studijni_oddeleni_RW

Ačkoliv je tento zaměstnanec definovaný na svém osobním PC *User*, má delegována práva nad *Organizační jednotkou* ***OU Students*** a velmi snadno - prostřednictvím *Console MMC* - spravuje studentské účty.



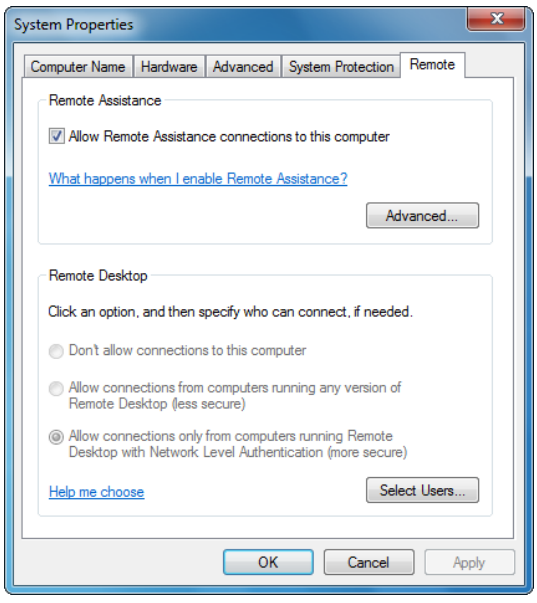
Obr. 45. Console MMC

12.2.10 Testování uživatele – Local Admin

Testovaný uživatel: Pavel Nejezchleb

- přihlašovací jméno: nejezchleb_pave
- členem skupin: gg_share_zamestnanci_RW

Lokální správci mají svůj osobní počítač pod plnou kontrolou s vyjímkou restrikcí, které jsou vynucené *Zásadami skupin (GPO)* - jednotný vzhled počítačového pozadí, spořič obrazovky chráněný heslem a needitovatelné povolení *Vzdálené plochy*.



Obr. 46. Remote Desktop

12.2.11 Testování – vzdálená instalace

Vzdálené instalaci s podporou *Zásad skupin* musí předcházet příprava instalačního balíčku *(*.msi)*. V našem případě byl takto zpracován souborový manažer Total Commander ver. 7 s přispěním software na tvorbu balíčků WinINSTALL LE ver. 10.

Aplikace politiky *u_install_total_commander_policy* cílené na uživatele (aktivované přihlášením daného uživatele do systému) prokázala, že lze vcelku jednoduše distribuovat software do koncových stanic s přispěním *GPO*.

12.2.12 Testování – hesla pro různé skupiny

Základní nastavení bezpečnosti z hlediska zásady hesel a uzamykání účtu pro běžné uživatele je nastaveno v *Defaul Domain Policy* a zahrnuje:

- Heslo musí splňovat požadavky na složitost – Povoleno,
- Maximální stáří hesla - 150 dnů,
- Minimální délka hesla - 10 znaků,
- Minimální stáří hesla - 5 dní,
- Vynutit použití historie hesel - 5 hesel zapamatováno,
- Doba uzamčení účtu - 30 minut,
- Prahová hodnota pro zamknutí účtu - 5 chybných pokusů o přihlášení.

Ve skupině *Studenti* dochází k „oslabení zabezpečení“ spočívající ve zkrácení minimální délky hesla na 8 znaků, naproti tomu u *IT Admin* dosáhneme zpřísnění zabezpečení prodloužením délky hesla na 20 znaků a prahové hodnoty pro zamknutí účtu na 2 chybné pokusy o přihlášení. Pro konfiguraci se použije *ADSI Edit*.

Testování potvrdilo funkčnost i této služby.

13 NÁVRH PROPOJENÍ NA OSTATNÍ SYSTÉMY

Minimální požadavek na sjednocení ostatních systémů s *Active Directory* je autentizace, dále pak schopnost kontrolovat provoz a řídit vynucování politik na základě identity uživatele.

13.1 STAG a MOODLE

Vzhledem k tomu, že systémy STAG a Moodle podporují *LDAP (Lightweight Directory Access Protocol)*, lze toto řešení použít pro autentizaci. Autorizace by vycházela z vlastních požadavků na jednotlivé systémy a vyžadovala by realizační zkušenost nebo čas pro vývoj.

13.2 SAP

Informační systém SAP podporuje *Single SignOn* s využitím *connectoru* (např. *SAP NetWeaver Management Console*), který provede autentizaci uživatele v *AD DS*. Autorizace je aplikována na úrovni IS SAP.

13.3 Antivirová kontrola

Významní hráči na trhu antivirových software využívají ve svých serverových aplikacích klíčové vlastnosti integrace *Active Directory Domain Services* a tím poskytují kontrolu nade všemi počítači umístěnými v doméně.

14 DOPORUČENÁ ŠKOLENÍ A CERTIFIKACE

Základem úspěšné implementace a další správy systému je tým vyškolených pracovníků se schopností předkládat taková řešení různých problémů, která budou zabezpečovat bezproblémové fungování *Microsoft Windows Server 2008 R2* a pracovních stanic na univerzitní síti. Je doporučené, aby správci sítě a pověření pracovníci měli možnost se účastnit odborných kurzů zaměřených na implementovaný systém u certifikovaných partnerů společnosti Misrosoft.

- **MOC6424 - Windows Server 2008 - základy Active Directory**
  - základní kurz - serverové role *AD DS* a jejich základní funkcionality.
- **MOC6425 - Windows Server 2008 - správa Active Directory**
  - konfigurace *AD DS* v distribuovaném prostředí, zavádění *GPO*, provádění záloh a obnov *AD DS*, monitoring
- **MOC6436 - Windows Server 2008 - plánování a optimalizace Active Directory**
  - rozšíření znalostí - schopnost plánovat a optimalizovat nasazení rozsáhlých sítí s *AD DS*.
- **MOC6432 - Windows Server 2008 - monitorování a údržba Active Directory**
  - správa a údržba doménového řadiče - zaměření na životní cyklus doménových řadičů, vytváření baseline, sledování serverů a jejich údržbu.
- **MOC6421 - Windows Server 2008 - správa síťových služeb**
  - konfigurace a řešení problémů síťové infrastruktury *WS 2008*.
- **MOC6435 - Windows Server 2008 - plánování a optimalizace síťových služeb**
  - rozšíření znalostí o principy návrhu a plánování implementace rozlehlých síťových řešeních na platformě *Microsoft Windows Server 2008*.
- **MOC6430 - Windows Server 2008 - plánování a správa serverů**
  - návrhový kurz - plánování implementace *Windows Server 2008 serverů*.
- **MOC6426 - Windows Server 2008 - správa ADFS, AD LDS, PKI a RMS**
  - správa a konfigurace nejvýznamnějších služeb *AD FS, AD LDS, RMS* a dalších postavených na *PKI* prostředí na platformě *Windows Server 2008*.
- **MOC6422 - Windows Server 2008 – virtualizace**
  - správa a řešení potíží virtuálního prostředí na platformě *Windows Server 2008* a *Hyper-V*.
- **MOC10215 - Windows Server Virtualization - nasazení a správa**

  - nasazení, nastavení, správa, sledování a řízení virtualizačních řešení postavených na platformě *Microsoft Hyper-V* a *System Center Virtual Machine Manager*.
- **MOC6428 - Windows Server 2008 - terminálové služby**
  - plánování, nasazení, údržba a řešení potíží při provozu terminálových služeb na platformě *Windows Server 2008*.
- **MOC6427 - Windows Server 2008 - správa Internet Information Services**
  - instalace, konfigurace, údržba - webový server *Internet Information Services 7.0* ve *Windows Serveru 2008*. [31]

Takto získané vědomosti lze zužitkovat při získávání certifikátů *Microsoft Certified Professional (MCP)*.

15 FINANCOVÁNÍ PROJEKTU

V rámci programového období 2007-2013 byla a stále je možnost financovat implementaci *Microsoft Windows Server 2008 R2* ze strukturálních fondů Evropské unie. Jelikož se jedná o investiční projekt, vzhledem k ceně hardwaru není vhodné využít programy dotací z Evropského sociálního fondu (ESF), ve kterých lze investice podpořit pouze v rámci křížového financování. Efektivnější je se soustředit na programy financované z Evropského fondu pro regionální rozvoj (ERDF).

V rámci ERDF lze získat dotaci například z následujících programů:

- Program přeshraniční spolupráce Slovenská republika - Česká republika 2007-2013,
- Operační program Výzkum a vývoj pro inovace,
- Operační program Podnikání a inovace.

15.1 Cenová nabídka

Popis	Množství	Jedn. cena
----- HW Domain Controllers -----		
HP ProLiant HP DL360G6 E5504, 4GB, 2x146GB	9	42 380,00
HP iLO Adv 1Svr incl 1yr TS&U SW	9	8 197,00
HP 460W HE 12V Hotplg AC Pwr Supply Kit	9	4 777,00
----- SW Microsoft -----		
Win Svr Std Win32 All Lang Lic/SA MVL	9	1 173,00
----- Práce -----		
Vstupní analýza, prováděcí projekt, realizace	počet čd[2]	20 900,00

[2] Je všeobecně doporučené, aby byl projekt implementován takovým partnerem, který je certifikován společností Microsoft a disponuje rozsáhlými zkušenostmi. V cenové nabídce je proto uvedena pouze jednotková cena za člověk/den, počet bude určen ze vstupních rozhovorů a prvotního sběru požadavků, do kterých jsou aktivně zapojeni jak klíčoví uživatelé, tak vedení univerzity.

ZÁVĚR

Každá počítačová síť je jako živý organismus, ve kterém proudí informace. Když implementujeme *Windows Server 2008 R2,* bude jeho srdcem *Active Directory Domain Services*. V distribuovaném výpočetním prostředí je tato rozšiřitelná adresářová služba, umožňující centrálně spravovat síťové prostředky s úzkou vazbou na nativní bezpečnostní funkce, velmi robustním a sofistikovaným nástrojem.

Cílem této práce bylo navrhnout implementaci *AD DS* do prostředí Univerzity Tomáše Bati ve Zlíně jako možnou alternativu morálně zastaralého síťového operačního systému *Novel Netware 6.5*.

Analýza přinesla celkový pohled na momentální stav sítě UTB ve Zlíně. Identifikuje síťovou architekturu včetně plánu IP adres a rozdělení aktivních prvků. Definuje síťové služby, *DNS*, *WINS*, *NTP*, *DHCP*, *PKI*, *WSUS*, centrální správu antiviru, elektronickou poštu a další neméně významné služby využívané UTB ve Zlíně a jejich použití. Dále vymezuje skupiny uživatelů na studenty a zaměstnance jednotlivých subjektů univerzity, přičemž lokální a síťoví administrátoři jsou zahrnuti do skupiny zaměstnanci.

Design *Active Directory Domain Services* se soustřeďuje na efektivní zpřístupnění adresářových informačních zdrojů a služeb prostřednictvím jednoho přihlášení koncovým uživatelům. Proto byla zvolena jednodoménová architektura s názvem *utb.local*, která ve svém důsledku podporuje i další rozvoj subdomén.

Rozdělení síťové infrastruktury do *Lokalit (Site)*, které obsahují referenci na *Podsítě (Subnets),* vycházejí ze současného plánu IP adres pro singulární objekty univerzity. Umístění *Doménových řadičů (Domain Controllers)* je těsně svázáno s *Lokalitami (Site)*, z tohoto důvodu byl do každé *Lokality* umístěn jeden *DC* s výjimkou site-u13 která je osazena *Hlavním operačním serverem (Operations Master)*, ke kterému je z hlediska další funkčnosti přiřazen redundantní *DC*.

Vzhledem ke skutečnosti, že byl návrh pojat jako stavba „na zelené louce“, jsou jeho součástí i jmenné konvence zahrnující *Lokality (Site)*, *Organizační jednotky (Organizational Unit)*, *Skupiny (Groups)*, a také názvy uživatelů, serverů a počítačů.

Základní členění *Organizačních jednotek (OU)* je cílené na jednotlivé fakulty a v další vrstvě na předpokládané rozložení na studenty, zaměstnance, lokální správce,

servery, sdílné tiskárny a počítačové stanice, které se v následující vrstvě dělí na učebny, uživatelské stanice a počítače lokálních administrátorů.

Zásady skupin (Group Policy) popisují doporučené politiky směrované jak na uživatele, tak na počítače a nechybí zde bezobslužná instalace s delegováním oprávnění.

Profily uživatele (*mandatorní* a *cestovní*) jsou uloženy na serveru v předem definovaném umístění, které určí správce.

DNS zóny jsou integrovány do *Active Directory Domain Services* s tím, že na všech *DC* je nastavena role *DNS* a *Servery pro předávání (Forwarders)* jsou lokalizovány na U13.

Instalace, konfigurace a testy probíhaly na virtuálních strojích zaručujících plnou funkčnost. Byly ověřeny základní funkcionality *AD DS* a pro restrikce byly připraveny scénáře směrované nejen na studenty, běžné uživatele, ale i na lokální administrátory. Výsledky testů potvrzují předpokládanou funkčnost.

Nasazením *Windows Serveru 2008 R2* lze získat opravdu robustní operační systém, podporující sítě nové generace, webové služby a aplikace. Zvláštní důraz je kladen na bezpečnostní a virtualizační technologie, škálovatelné funkce, vzdálené přístupy a nižší spotřebu energie v přímém kontextu se správou celého systému, která podtrhuje technologickou vyspělost celého systému.

ZÁVĚR V ANGLIČTINĚ

Every single computer network may sound like a live organism inside which information flow. When it comes to *Windows Server 2008 R2* implementation *Active Directory Domain Services* will become its heart. In the distribution computing environment you may find this extendable directory service - providing us a central maintenance of the network tooling with a close bond to native security functions – as a truly robust and sophisticated tool.

The target of this work is anl implementation proposal of *AD DS* into Tomas Bata University in Zlin as an alternative to morally older *Novel Netware 6,5* network operation system.

The analysis has given us an overall look into status of UTB Zlin network. We identify the network architecture including IP address plan and active elements split. We define network services, *DNS*, *WINS*, *NTP*, *DHCP*, *PKI*, *WSUS*, a central antivirus maintenance, electronic mailing as well as various other significant services utilized at UTB in Zlin and their purpose of use. Further it determines groups of users selecting them in between students and employees of particular university subjects whereas local and network administrators belong to the group with employees.

Design *Active Directory Domain Services* is focused on accessibility effectiveness of information resources and services through a single login by the end users. That is why a single domain architecture was set up under *utb.local* name which in its own consequence even supports the subsequent sub-domains development.

The network infrastructure splitting into *Site* which contain a reference to *Subnets* come out of current IP address plan set for singular objects of the University. Location of *Domain Controllers* is closely linked with *the Sites*. From this reason there was a single *DC* installed with each *the Site* with an exception of site-u13 that is provided with the *Operation Master* to which there is a redundant *DC* allocated from further utility point of view.

Owing to the fact that the solution was taken as construction “in a green field” nominal conventions including *Sites*, *Organizational Units*, *Groups* as well as names of users, servers and computers are considered as its parts.

The basic division of *OU* is targeted at particular faculties and in the next layer at supposed distribution to students, employees, local administrators, servers, shared printers and computer stations which, in the following layer, are divided into classrooms, users' stations and local administrators' computers.

Group Policy principles describe recommended politicians directed to the both users and computers and one will not also miss a control free installation with an authorization delegation.

User's profiles (*mandatory* as well as *traveling*) are saved on server in in-advance defined location determined by administrator.

DNS zones are integrated into *Active Directory Domain Policy* with a condition that with all the *DC*s there is a role of *DNS* set up and servers to *Forwarding* are located on U13.

Installation, configuration and test sessions ran on virtual machines securing entire utilization. *AD DS* basic functionality were verified and in terms of restrictions there were scenarios ready and directed not only onto students however ordinary users and local administrators as well. The test session results prove supposed utilization.

Using *Windows Serveru 2008 R2* there can be achieved a really robust operational system supporting networks of new generation, website services and applications. Special emphasis is put on security and virtual-like technology, spectrum utility, remote accesses and lower consumption of electrical energy in direct context with administration of the whole system which underlines technological maturity of the entire system.

SEZNAM POUŽITÉ LITERATURY

[1] *Windows Server 2008 R2 : Získejte odpovědi na dotazy týkající se systému Windows Server 2008.* [online]. 2010 [cit. 2010-04-21]. Dostupné z WWW: <http://www.microsoft.com/cze/windowsserver2008/faq.mspx>

[2] RUSSEL, Charlie, CRAWFORD, Sharon. *Microsoft Windows Server 2008 : Velký průvodce administrátora.* Brno: Computer Press a.s., 2009. 1271 s. ISBN 978-80-251-2115-3

[3] REIMER, Stan, KEZEMA, Conan, MULCARE, Mike. *Windows Server 2008 Active Directory : Resource Kit*. Redmond, Washington: Microsoft Press, 2008. 827 s. ISBN 2008920569.

[4] ŠEVEČEK, Ondřej. Er dvojka a novinky v Active Directory : Přehled novinek. *Microsoft Technet Blog CZ/SK* [online]. 2009, no. 1, [cit. 2010-04-26]. Dostupný z WWW: <http://blogs.technet.com/technetczsk/pages/er-dvojka-a-novinky-v-active-directory.aspx>.

[5] PAVLIS, Martin. Active Directory v podání Windows Server 2008. *Konzultant.NET* [online]. 1.11.2008, n, [cit. 2010-04-26]. Dostupný z WWW: <http://www.konzultant.net/a35-Active-Directory-v-podani-Windows-Server-2008.aspx>.

[6] ČERNOVSKÝ, Roman. Novinky v Active Directory v serveru Windows Serveru 2008 v kostce. *Microsoft Technet Blog CZ/SK* [online]. 2007, n, [cit. 2010-04-26]. Dostupný z WWW: <http://blogs.technet.com/technetczsk/archive/2007/09/20/novinky-AD-serveru-windows-serveru-2008-v-kostce.aspx>.

[7] Požadavky na systém Windows Server 2008 R2. In *Windows Server 2008 R2*. [s.l.] : [s.n.], 2010 [cit. 2010-04-26]. Dostupné z WWW: <http://www.microsoft.com/cze/windowsserver2008/system-requirements.mspx>.

[8] Přehled edic. In *Windows Server 2008 R2*. [s.l.] : [s.n.], 2010 [cit. 2010-04-26]. Dostupné z WWW: <http://www.microsoft.com/cze/windowsserver2008/r2-editions-overview.mspx>.

[9] STANEK, William R. *Microsoft Windows Server 2008 : Kapesní rádce administrátora*. Brno: Computer Pess a.s., 2008. 704 s. ISBN 978-80-251-1936-5.

[10] MCLEAN, Ian; THOMAS, Orin. *Windows Server Administration : Self-Paced Training Kit*. Redmond: Microsoft Press, 2008. 768 s. ISBN X14-33190.

[11] HOLME, Dan, RUEST, Nelson, RUEST, Danielle. Configuring Windows Server 2008 Active Directory : Training Kit. Redmond, Washington: Microsoft Press, 2008. 951 s. ISBN X14-15141.

[12] STANEK, William R. *Mistrovství v Microsoft Windows Server 2008*. Brno: Computer Press a.s., 2009. 1368 s. ISBN 978-80-251-2158-0.

[13] Microsoft Corporation. *6424A Fundamentals of Windows Server 2008 Active Directory* : Microsoft Official Course. [s.l.] : [s.n.], 2008. 320 s. ISBN X14-69071.

[14] Microsoft Corporation. *6425A Configuring and Troubleshooting Windows Server 2008 Active Directory Domain Services* : Microsoft Official Course. [s.l.] : [s.n.], 2008. 800 s. ISBN X14-69064.

[15] STANEK, William R. *Active Directory : Kapesní rádce administrátora*. první vydání. Brno: Computer Pess a.s., 2009. 352 s. ISBN 978-80-251-2555-7.

[16] THOMAS, Orin, et al. *Windows Server Enterprise Administration : Self-Paced Training Kit*. Redmond: Microsoft Press, 2008. 572 s. ISBN X14-37560.

[17] HOLME, Dan. *Windows Administration : Productivity Solutions for IT Professionals - Resource Kit*. Redmond: Microsoft Press, 2008. 710 s. ISBN X14-38533.

[18] PRICE, Brad. *Active Directory : Optimální postupy a řešení*. Brno : Computer Press a.s., 2005. 381 s. ISBN 80-251-0602-0.

[19] MAR-ELIA, Darren, MELBER, Derek, STANEK, Wiliam S. *Zásady skupin Microsoft Windows: Microsoft Windows Group Policy Guide*. Brno: Computer Press a.s., 2006. 760 s. ISBN 80-251-1261-4.

[20] STANEK, William R. *Group Policy - Zásady skupiny ve Windows: Kapesní rádce administrátora*. Brno: Computer Press a.s., 2010. 351 s. ISBN 978-80-251-2920-3.

[21] *Microsoft Technet* [online]. 2010 [cit. 2010-04-28]. Role Globálního katalogu. Dostupné z WWW: <http://technet.microsoft.com/cs-cz/library/cc736934%28WS.10%29.aspx>.

[22] *IT Bloguje* [online]. 2009 [cit. 2010-04-28]. Služba Global Catalog na DC Serveru. Dostupné z WWW: <http://www.it-bloguje.cz/certifikace/veobecna-teorie/24-zapnuti-nebo-vypnuti-sluby-global-catalog-na-domain-controller-serveru.html>.

[23] ČERNOVSKÝ, Roman. *Microsoft Technet* [online]. 2007 [cit. 2010-04-28]. Windows Server 2008 a doménový řadič jen pro čtení. Dostupné z WWW: <http://blogs.technet.com/technetczsk/archive/2007/05/28/windows-server-2008-RODC.aspx>.

[24] *Wikipedia* [online]. 2010 [cit. 2010-04-28]. Flexible single master operation. Dostupné z WWW: <http://en.wikipedia.org/wiki/Flexible_single_master_operation>.

[25] SPURNÁ, Ivana. *Mgr. Ivana Spurna* [online]. 2003 [cit. 2010-04-29]. :: 28. Skupiny. Dostupné z WWW: <http://www.ivasp.info/pages/technicke-vybaveni-3/technicke-vybaveni-3-28kap.php>.

[26] KNOTEK, Miroslav. *Konzultant NET* [online]. 25.7.2007 [cit. 2010-04-29]. Správa nejen bezpečnostních aktualizací pomocí WSUS 3.0. Dostupné z WWW: <http://www.konzultant.net/a6-Sprava-nejen-bezpecnostnich-aktualizaci-pomoci-WSUS-3-0.aspx>.

[27] *Microsoft Security Response Center* [online]. 2010 [cit. 2010-04-29]. Microsoft Security Response Center. Dostupné z WWW: <Microsoft Security Response Center>.

[28] FRK, Bohuslav. Automatizací instalací ku pomoci: Na aplikace bezobslužně i v doméně. *Connect*. Prosinec 2009, 12/2008, s. 46-47.

[29] Microsoft Corporation. *6421A Configuring and Troubleshooting Windows Server 2008 Network Infrastructure* : Microsoft Official Course. [s.l.] : [s.n.], 2008. 900 s. ISBN X14-69052.

[30] NORTHRUP, Tony; MACKIN, J.C. *Configuring Windows Server 2008 Network Infrastructure : Self-Paced Training Kit*. Redmond: Microsoft Press, 2008. 657 s. ISBN X14-33192.

[31] Nabídka kurzů [online]. 2010 [cit. 2010-04-30]. Gopas. Dostupné z WWW: <http://www.gopas.cz/SeznamOblasti.aspx>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Services
AD LDS	Active Directory Lightweight Directory Services
AD RMS	Active Directory Rights Management Services
CD	Compact Disc
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EFS	Encrypting File System
ERDF	European Regional Development Fun
ESF	Evropský sociální fond
FAI	Fakulta aplikovane informatiky
FSMO	Flexible Single Master of Operation
GC	Global Catalog
GPO	Group Policy
GUID	Globally Unique Identifier
HP	Hewlett-Packard
HW	Hardware
IE	Internet Explorer
IP	Internet Protocol
IPsec	Internet Protocol Security
IS	Informační systém
IT	Information Technology
KCC	Knowledge Consistency Checker

LDAP	Lightweight Directory Access Protocol
MCP	Microsoft Certified Professional
MMC	Microsoft Management Console
MSRC	Microsoft Security Response Center
NAP	Network Access Protection
NTP	Network Time Protocol
OU	Organizational Unit
PC	Personal Computer
PKI	Public Key Infrastructure
R	Read
RAM	Random-Access Memory
RODC	Read Only Domain Controller
SID	Security Identifiers
SW	Software
VGA	Video Graphics Array
VPN	Virtual Private Network
W	Write
WS	Windows Server
WSUS	Windows Server Update Services

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

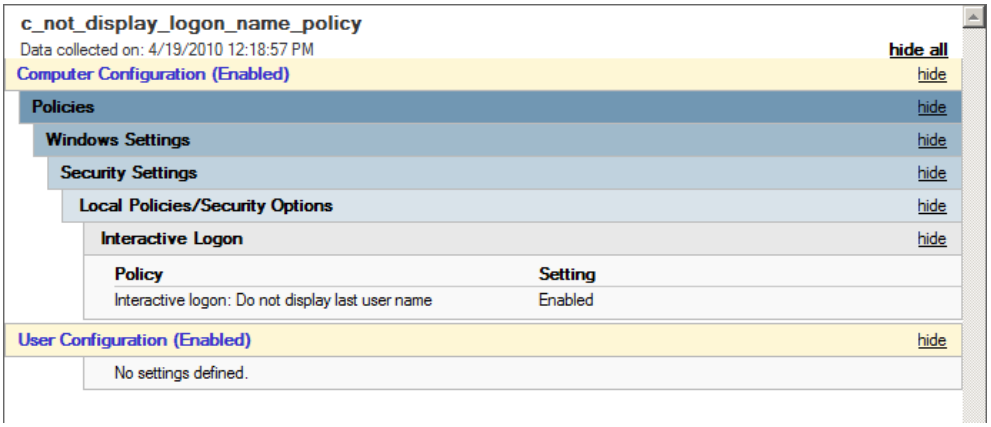
SEZNAM PŘÍLOH

PŘÍLOHA P II: SEZNAM SUBNETŮ

Název Subnet	Adresní blok
site-u1 **nám. T. G. Masaryka 275** **Zlín**	10.1.0.0/24 10.1.8.0/22 10.1.16.0/24 10.1.128.0/24 10.1.130.0/24 10.1.136.0/24
site-u2 **Mostní 5139** **Zlín**	10.2.0.0/24 10.2.8.0/22 10.2.16.0/23 10.2.128.0/24 10.2.130.0/24 10.2.136.0/24
site-u4 **Štefánikova 2431** **Zlín**	10.4.0.0/24 10.4.8.0/22 10.4.16.0/23 10.4.128.0/24 10.4.130.0/24 10.4.136.0/24
site-u5 **Jižní svahy** **Nad stráněmi 4511** **Zlín**	10.5.0.0/24 10.5.8.0/22 10.5.16.0/23 10.5.128.0/24 10.5.130.0/24 10.5.136.0/24
site-u10 **nám. T. G. Masaryka 1279** **Zlín**	10.10.0.0/24 10.10.8.0/22 10.10.16.0/23 10.10.128.0/24 10.10.130.0/24 10.10.136.0/24
site-u11 **Nad Ovčírnou 3685** **Zlín**	10.10.0.0/24 10.10.8.0/22 10.10.16.0/23 10.10.128.0/24

Název Subnet	Adresní blok
	10.10.130.0/24 10.10.136.0/24
site-u13 **nám. T. G. Masaryka 5555** **Zlín**	10.13.0.0/24 10.13.8.0/22 10.13.16.0/22 10.13.128.0/24 10.13.130.0/24 10.13.136.0/24
site-uh **Studentské nám. 1532** **Uherské Hradiště**	10.13.0.0/24 10.13.8.0/22 10.13.16.0/22 10.13.128.0/24 10.13.130.0/24 10.13.136.0/24

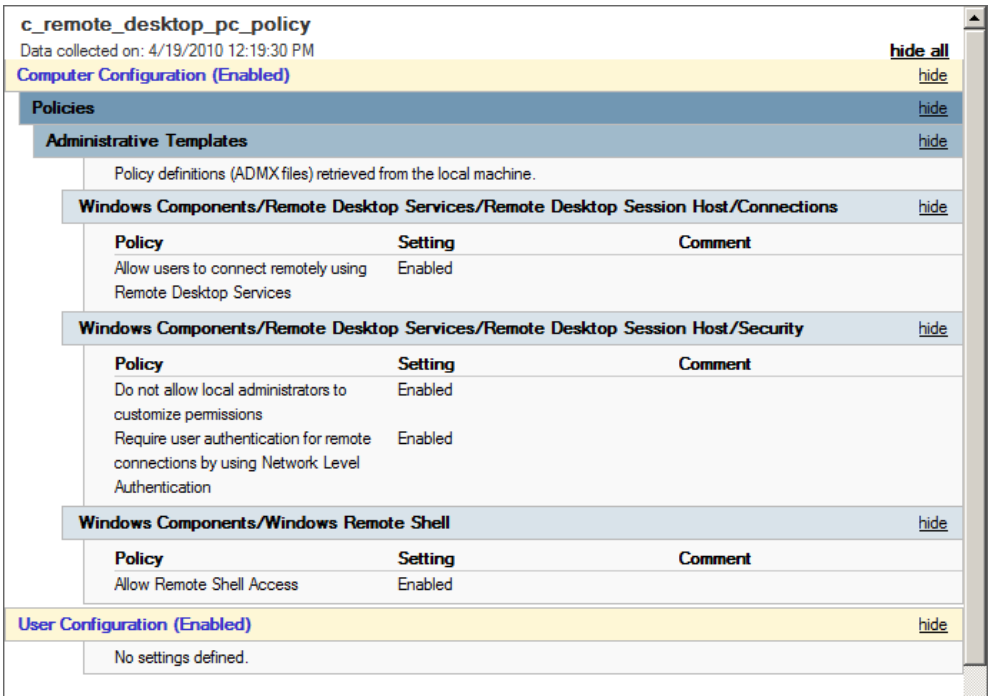
PŘÍLOHA P III: ZÁSADY SKUPIN - NASTAVENÍ



c_not_display_logon_name_policy
Data collected on: 4/19/2010 12:18:57 PM — hide all
Computer Configuration (Enabled) — hide
Policies — hide
Windows Settings — hide
Security Settings — hide
Local Policies/Security Options — hide
Interactive Logon — hide

Policy	Setting
Interactive logon: Do not display last user name	Enabled

User Configuration (Enabled) — hide
No settings defined.



c_remote_desktop_pc_policy
Data collected on: 4/19/2010 12:19:30 PM — hide all
Computer Configuration (Enabled) — hide
Policies — hide
Administrative Templates — hide
Policy definitions (ADMX files) retrieved from the local machine.
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections — hide

Policy	Setting	Comment
Allow users to connect remotely using Remote Desktop Services	Enabled	

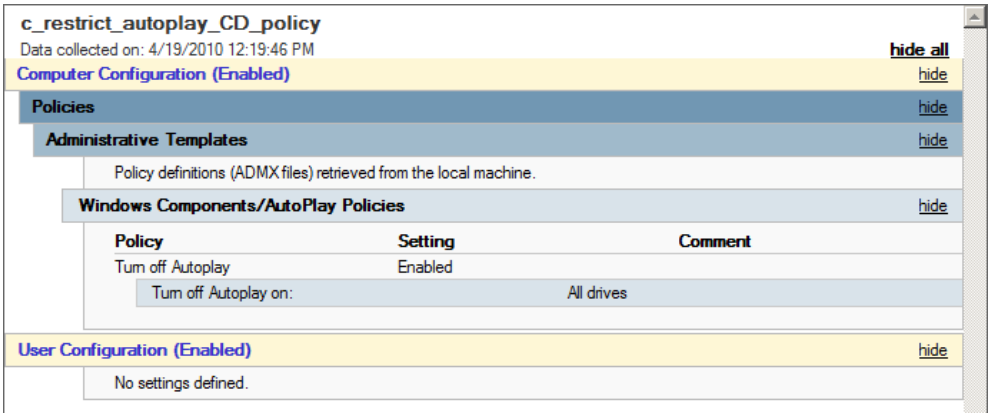
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security — hide

Policy	Setting	Comment
Do not allow local administrators to customize permissions	Enabled	
Require user authentication for remote connections by using Network Level Authentication	Enabled	

Windows Components/Windows Remote Shell — hide

Policy	Setting	Comment
Allow Remote Shell Access	Enabled	

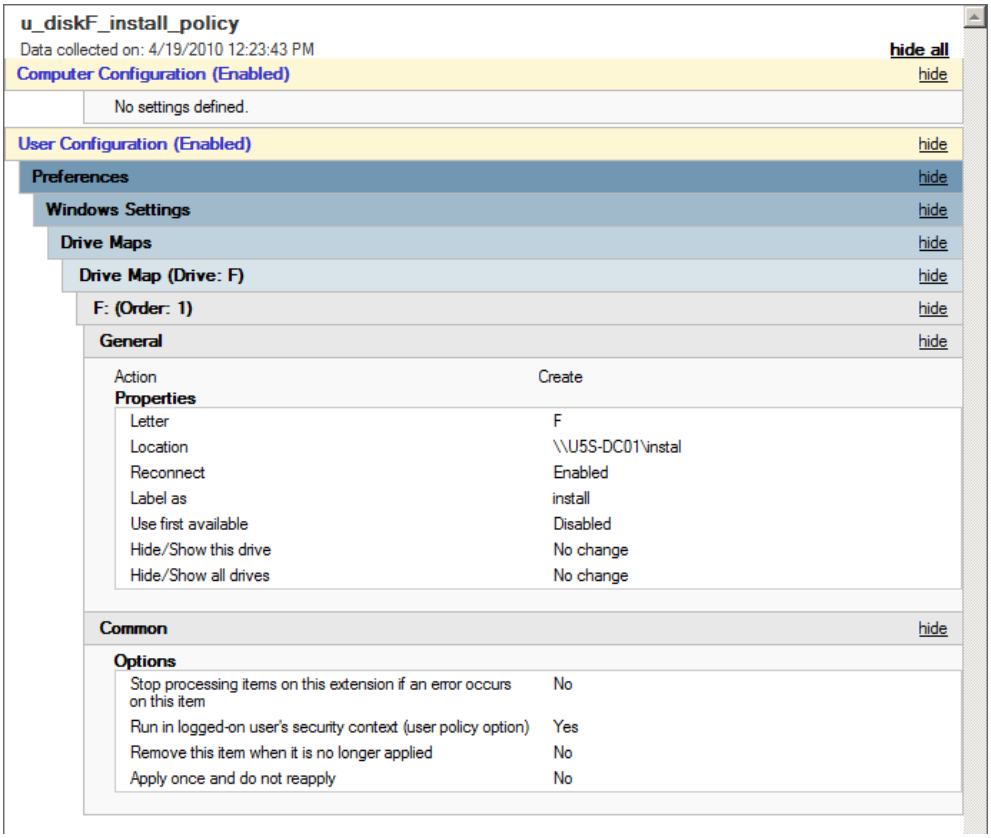
User Configuration (Enabled) — hide
No settings defined.



c_restrict_autoplay_CD_policy
Data collected on: 4/19/2010 12:19:46 PM — hide all
Computer Configuration (Enabled) — hide
Policies — hide
Administrative Templates — hide
Policy definitions (ADMX files) retrieved from the local machine.
Windows Components/AutoPlay Policies — hide

Policy	Setting	Comment
Turn off Autoplay	Enabled	
Turn off Autoplay on:	All drives	

User Configuration (Enabled) — hide
No settings defined.



u_diskF_install_policy

Data collected on: 4/19/2010 12:23:43 PM

hide all

Computer Configuration (Enabled) hide

No settings defined.

User Configuration (Enabled) hide

Preferences hide

Windows Settings hide

Drive Maps hide

Drive Map (Drive: F) hide

F: (Order: 1) hide

General hide

Action	Create

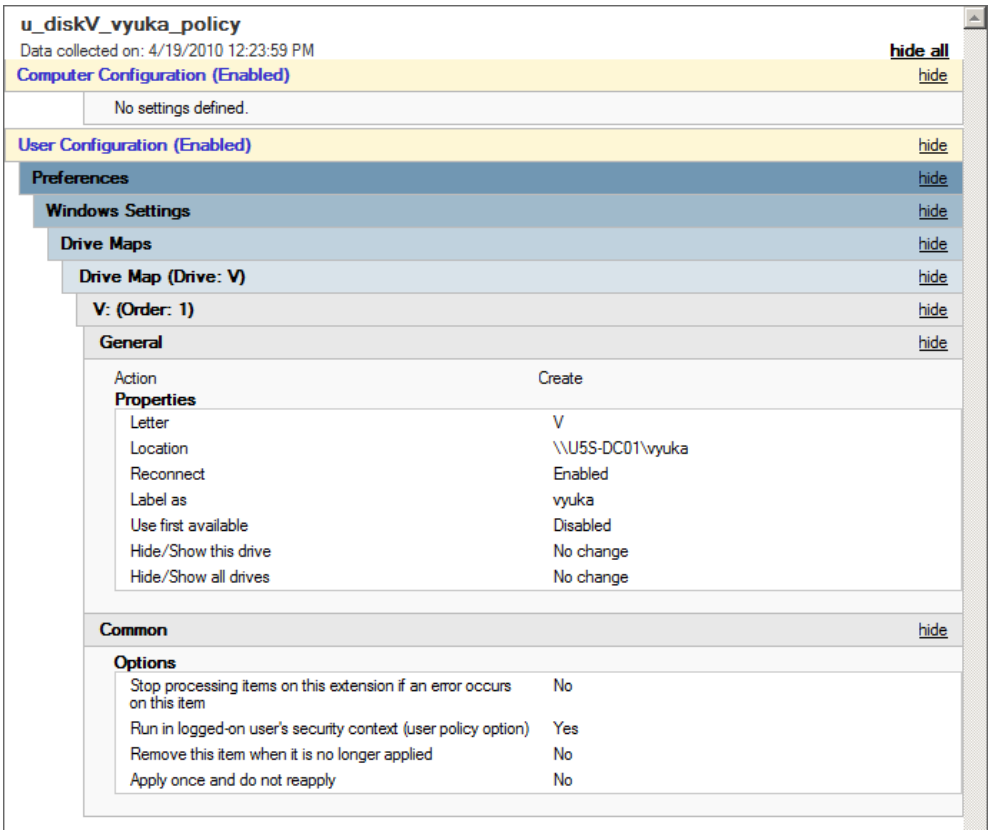
Properties

Letter	F
Location	\\U5S-DC01\instal
Reconnect	Enabled
Label as	install
Use first available	Disabled
Hide/Show this drive	No change
Hide/Show all drives	No change

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	Yes
Remove this item when it is no longer applied	No
Apply once and do not reapply	No



u_diskV_vyuka_policy

Data collected on: 4/19/2010 12:23:59 PM

hide all

Computer Configuration (Enabled) hide

No settings defined.

User Configuration (Enabled) hide

Preferences hide

Windows Settings hide

Drive Maps hide

Drive Map (Drive: V) hide

V: (Order: 1) hide

General hide

Action	Create

Properties

Letter	V
Location	\\U5S-DC01\vyuka
Reconnect	Enabled
Label as	vyuka
Use first available	Disabled
Hide/Show this drive	No change
Hide/Show all drives	No change

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	Yes
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

u_diskX_fai_policy

Data collected on: 4/19/2010 12:24:14 PM

hide all

Computer Configuration (Enabled) hide

No settings defined.

User Configuration (Enabled) hide

Preferences hide

Windows Settings hide

Drive Maps hide

Drive Map (Drive: X) hide

X: (Order: 1) hide

General hide

Action	Create

Properties

Letter	X
Location	\\U5S-DC01\fai
Reconnect	Enabled
Label as	FAI Office work
Use first available	Disabled
Hide/Show this drive	No change
Hide/Show all drives	No change

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	Yes
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

u_IE_allow_file_download_policy

Data collected on: 4/19/2010 12:24:30 PM

hide all

Computer Configuration (Enabled) hide

No settings defined.

User Configuration (Enabled) hide

Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local machine.

Windows Components/Internet Explorer/Internet Control Panel/Security Page hide

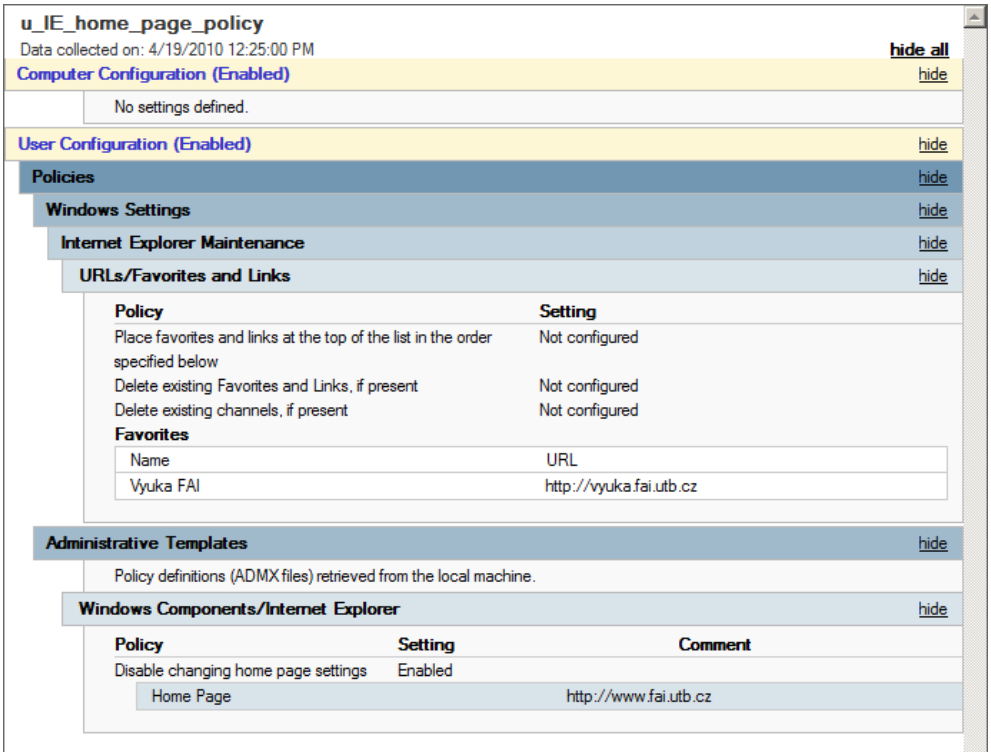
Policy	Setting	Comment
Site to Zone Assignment List	Enabled	

Enter the zone assignments here.	
http://www.utb.cz	2
http://vyuka.fai.utb.cz	1
http://fai.utb.cz	2

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Internet Zone hide

Policy	Setting	Comment
Allow file downloads	Enabled	

Allow file downloads	Disable



u_IE_home_page_policy

Data collected on: 4/19/2010 12:25:00 PM

hide all

Computer Configuration (Enabled) hide

No settings defined.

User Configuration (Enabled) hide

Policies hide

Windows Settings hide

Internet Explorer Maintenance hide

URLs/Favorites and Links hide

Policy	Setting
Place favorites and links at the top of the list in the order specified below	Not configured
Delete existing Favorites and Links, if present	Not configured
Delete existing channels, if present	Not configured

Favorites

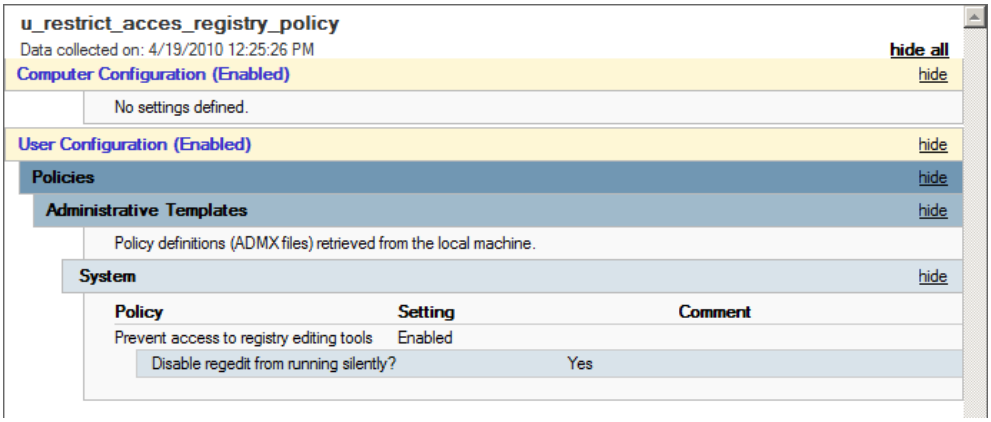
Name	URL
Vyuka FAI	http://vyuka.fai.utb.cz

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local machine.

Windows Components/Internet Explorer hide

Policy	Setting	Comment
Disable changing home page settings	Enabled	
Home Page	http://www.fai.utb.cz	



u_restrict_acces_registry_policy

Data collected on: 4/19/2010 12:25:26 PM

hide all

Computer Configuration (Enabled) hide

No settings defined.

User Configuration (Enabled) hide

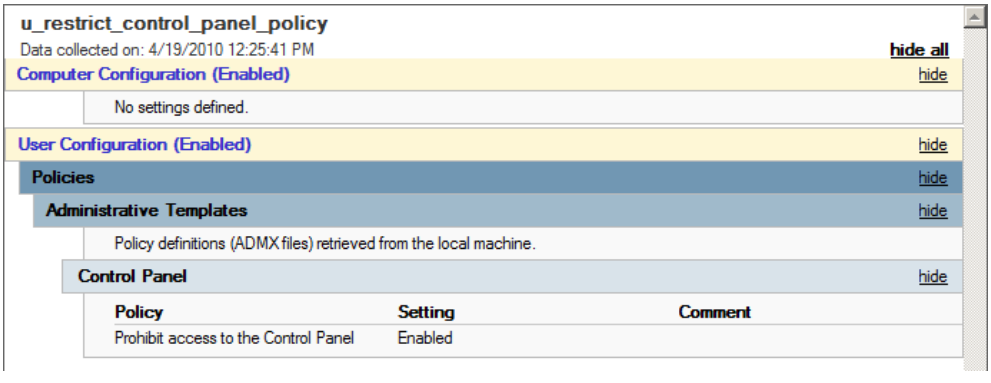
Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local machine.

System hide

Policy	Setting	Comment
Prevent access to registry editing tools	Enabled	
Disable regedit from running silently?	Yes	



u_restrict_control_panel_policy

Data collected on: 4/19/2010 12:25:41 PM

hide all

Computer Configuration (Enabled) hide

No settings defined.

User Configuration (Enabled) hide

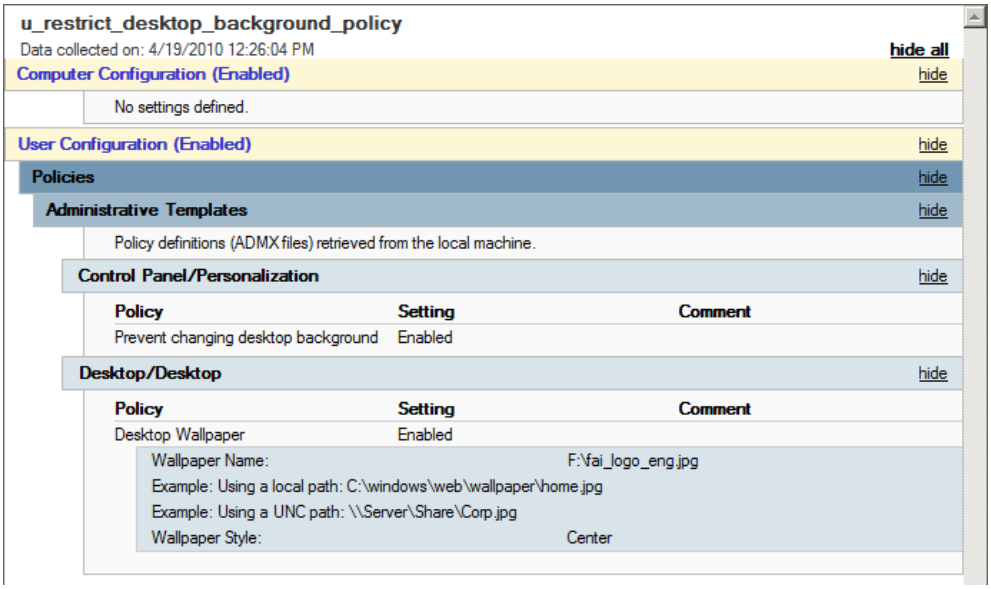
Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local machine.

Control Panel hide

Policy	Setting	Comment
Prohibit access to the Control Panel	Enabled	



u_restrict_desktop_background_policy

Data collected on: 4/19/2010 12:26:04 PM

hide all

Computer Configuration (Enabled) hide

No settings defined.

User Configuration (Enabled) hide

Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local machine.

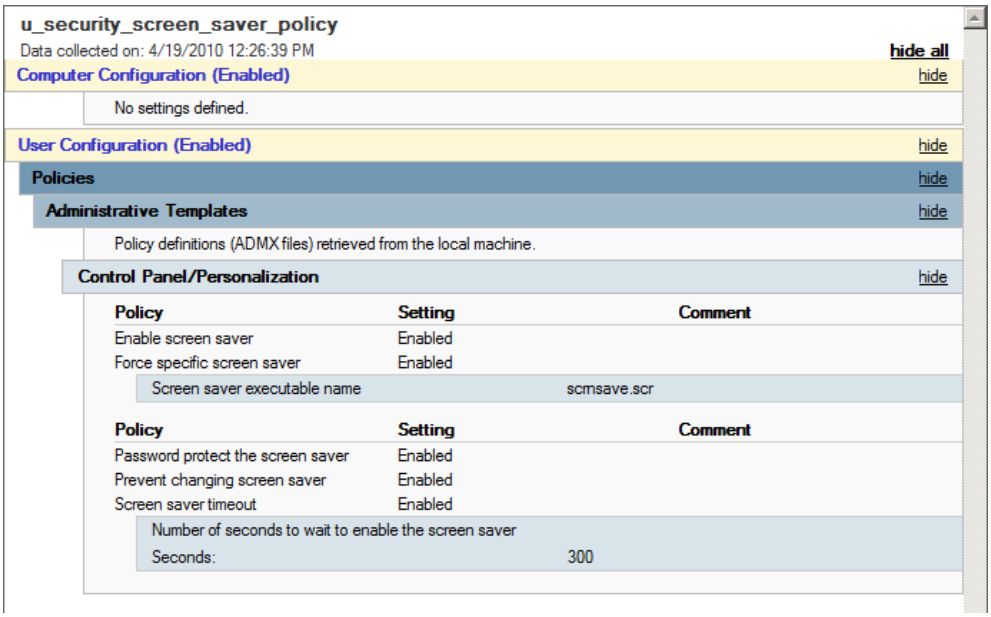
Control Panel/Personalization hide

Policy	Setting	Comment
Prevent changing desktop background	Enabled	

Desktop/Desktop hide

Policy	Setting	Comment
Desktop Wallpaper	Enabled	

Wallpaper Name:	F:\fai_logo_eng.jpg
Example: Using a local path: C:\windows\web\wallpaper\home.jpg	
Example: Using a UNC path: \\Server\Share\Corp.jpg	
Wallpaper Style:	Center



u_security_screen_saver_policy

Data collected on: 4/19/2010 12:26:39 PM

hide all

Computer Configuration (Enabled) hide

No settings defined.

User Configuration (Enabled) hide

Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local machine.

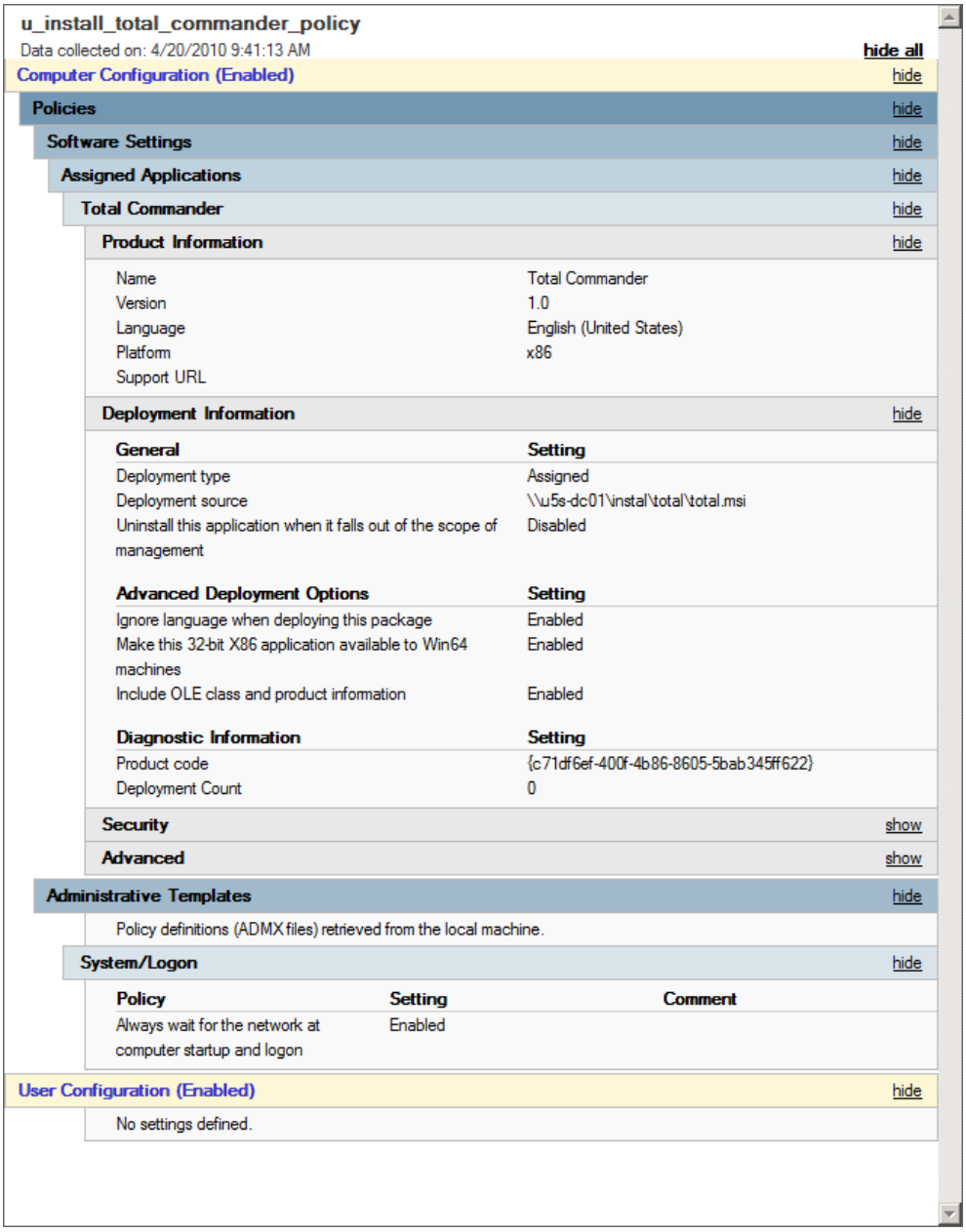
Control Panel/Personalization hide

Policy	Setting	Comment
Enable screen saver	Enabled	
Force specific screen saver	Enabled	

Screen saver executable name	scrnsave.scr

Policy	Setting	Comment
Password protect the screen saver	Enabled	
Prevent changing screen saver	Enabled	
Screen saver timeout	Enabled	

Number of seconds to wait to enable the screen saver	
Seconds:	300



u_install_total_commander_policy

Data collected on: 4/20/2010 9:41:13 AM

hide all

Computer Configuration (Enabled) hide

Policies hide

Software Settings hide

Assigned Applications hide

Total Commander hide

Product Information hide

Name	Total Commander
Version	1.0
Language	English (United States)
Platform	x86
Support URL	

Deployment Information hide

General	Setting
Deployment type	Assigned
Deployment source	\\u5s-dc01\instal\total\total.msi
Uninstall this application when it falls out of the scope of management	Disabled

Advanced Deployment Options	Setting
Ignore language when deploying this package	Enabled
Make this 32-bit X86 application available to Win64 machines	Enabled
Include OLE class and product information	Enabled

Diagnostic Information	Setting
Product code	{c71df6ef-400f-4b86-8605-5bab345ff622}
Deployment Count	0

Security show

Advanced show

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local machine.

System/Logon hide

Policy	Setting	Comment
Always wait for the network at computer startup and logon	Enabled	

User Configuration (Enabled) hide

No settings defined.