Zabezpečení v prostředí Microsoft Active Directory

Karol VAIT

Bakalářská práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Karol Vait**
Osobní číslo:	**A14172**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Zabezpečení v prostředí Microsoft Active Directory**
Téma anglicky:	**Microsoft Active Directory Security**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Připojte tenkého klienta do domény.**
3. **Nastavte zabezpečení a jednotné prostředí všech klientů.**
4. **Popište a využijte možnosti centralizované správy.**
5. **Věnujte se zabezpečení a správě citlivých dat.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ANDERSON, Christa a Kristin L. GRIFFIN. Windows Server 2008 R2 Remote Desktop Services Resource Kit. Redmond, Washington: Microsoft Press, 2010. ISBN 9780735627376.**
2. **DESMOND, Brian, Joe RICHARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. Active Directory: Designing, Deploying, and Running Active Directory. 5'th. United States of America: O'Reilly Media, 2013. ISBN 978-1-449-32002-7.**
3. **MOSKOWITZ, Jeremy. Group Policy: Fundamentals, Security, and the Managed Desktop. 3'rd. Indianapolis, Indiana: John Wiley & Sons, 2015. ISBN 978-1-119-03558-9.**
4. **WRIGHT, Byron a Brian SVIDERGOL. Virtualizing Desktops & Apps with Windows Server 2012 R2 Inside Out. 1'st. Redmond, Washington: Microsoft Press, 2015. ISBN 978-0-7356-9721-8.**
5. **SMITH, Russell. Least Privilege Security for Windows 7, Vista and XP. 1'st. Olton, Birmingham: Packt Publishing, 2010. ISBN 978-1-849680-04-2.**

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

Datum zadání bakalářské práce: **3. února 2017**

Termín odevzdání bakalářské práce: **29. května 2017**

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

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

Ing. Jan Valouch, Ph.D.
ředitel ústavu

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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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, dne …….

podpis diplomanta

ABSTRAKT

Táto bakalárska práca sa zaoberá vybranými možnosťami zabezpečenia v prostredí Microsoft Active Directory. Cieľom práce je najprv teoreticky popísať a neskôr aj ukázať na reálnych príkladoch, ako je možné prostredníctvom Adresárových služieb, Služieb vzdialenej plochy a Tenkého klienta, vytvoriť bezpečné a jednoducho centrálne spravované prostredie, vhodné napríklad pre nasadenie do výrobného podniku.

Kľúčové slová: Adresárová služba, Skupinové politiky, Windows server, Služby vzdialenej plochy, Tenký klient

ABSTRACT

This bachelor thesis covers selected options to improve security in Microsoft Active Directory environment. The aim of this thesis is to explain and demonstrate practical application of Directory services, Remote Desktop Services and Thin clients to create a secure and centrally managed environment suitable, for example for Manufacturing corporation.

Keywords: Active Directory, Group policy, Windrows server, Remote Desktop Services, Thin client

Poďakovanie

Rád by som sa poďakoval vedúcemu mojej bakalárskej práce pánovi doc. Ing. Martinovi Syslovi, Ph.D., za jeho podnetné rady a pripomienky a mojej žene Kristíne za morálnu podporu pri mojom štúdiu ...

Motto:

„Je iba jediná prekážka na dosiahnutie tvojho cieľa – ty sám.“

neznámy

OBSAH

ÚVOD **9**

I TEORETICKÁ ČASŤ **10**

1 MICROSOFT WINDOWS SERVER 2012 R2 ..... **11**

1.1 PREHĽAD EDÍCIÍ A ICH POROVNANIE 11

1.2 NOVINKY VO WINDOWS SERVER 2012 R2 12

1.2.1 RDS 12

1.3 LICENCOVANIE 14

1.4 HARDVÉROVÉ POŽIADAVKY 14

2 ACTIVE DIRECTORY DOMAIN SERVICES (AD DS) **15**

2.1 FYZICKÁ ŠTRUKTÚRA 15

2.1.1 DOMÉNOVÉ RADIČE (DOMAIN CONTROLLERS) 15

2.1.2 ACTIVE DIRECTORY LOKALITA (ACTIVE DIRECTORY SITE) 16

2.1.3 ACTIVE DIRECTORY PARTICIE (ACTIVE DIRECTORY PARTITIONS) 16

2.2 LOGICKÁ ŠTRUKTÚRA 17

2.2.1 DOMÉNA (DOMAIN) 17

2.2.2 STROM (TREE) 18

2.2.3 LES (FOREST) 18

2.2.4 ROLA HLAVNÉHO OPERAČNÉHO SERVERA (FSMO) 19

2.2.5 ORGANIZAČNÉ JEDNOTKY (OU) 21

2.2.6 SKUPINY 22

2.2.6.1 Typy skupín 22

2.2.6.2 Rozsah skupín 22

2.2.6.3 Odporúčaný model použitia 23

2.2.7 ĎALŠIE DÔLEŽITÉ OBJEKTY 24

2.2.7.1 Užívateľ (User) 24

2.2.7.2 Počítač (Computer) 24

2.2.7.3 Zdieľaný priečinok (Share) 25

2.2.7.4 Tlačiareň (Printer) 25

2.2.8 SKUPINOVÉ POLITIKY (GROUP POLICY) 25

2.2.8.1 Nastavenia aplikované na Počítač (Computer Configuration) 27

2.2.8.2 Nastavenia aplikované na užívateľa (User Configuration) 27

2.2.8.3 Spôsob Aplikovania politík 28

2.2.8.4 Applocker 28

2.3 ĎALŠIE MOŽNOSTI ZABEZPEČENIA 30

2.3.1 DELEGOVANIE PRÁVOMOCÍ 30

2.3.2 UŽÍVATEĽSKÉ HESLÁ 30

2.3.3 AUDITING A PROTOKOLY UDALOSTÍ 31

2.3.4 ZABEZPEČENIE LOGICKÉHO PRÍSTUPU 31

2.3.5 ZABEZPEČENIE DÁT 32

3 UŽÍVATEĽSKÉ PROFILY **34**

3.1 TYPY UŽÍVATEĽSKÝCH PROFILOV 34

4 SLUŽBY VZDIALENEJ PLOCHY (RDS) 35
5 OSTATNÉ DÔLEŽITÉ ROLE A SLUŽBY 38
5.1 DOMAIN NAME SYSTEM (DNS) 38
5.2 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) 38
5.3 SÚBOROVÉ A TLAČOVÉ SLUŽBY (FILE AND PRINT SERVICES) 38
5.4 WINDOWS SERVER UPDATE SERVICES (WSUS) 38
6 KLIENTSKÁ STANICA (TENKÝ KLIENT) 39
II PRAKTICKÁ ČASŤ 41
7 POPIS SÚČASNÉHO STAVU 42
7.1 ORGANIZAČNÁ ŠTRUKTÚRA SPOLOČNOSTI 42
7.2 HW INFRAŠTRUKTÚRA SPOLOČNOSTI 43
7.3 ZOZNAM SERVEROV A SLUŽIEB 44
7.4 SIEŤOVÁ TOPOLÓGIA 44
8 CIELE NÁVRHU A POŽIADAVKY SPOLOČNOSTI 45
9 NASADENÉ RIEŠENIE 46
9.1 SÚBOROVÝ SERVER 46
9.2 RDS SERVER 47
9.2.1 HARDVÉROVÉ PARAMETRE A POUŽITÉ LICENCIE 47
9.3 AD INFRAŠTRUKTÚRA 48
9.4 DOMÉNOVÁ SKUPINOVÁ POLITIKA – RDS SETTINGS 49
9.4.1 KONFIGURÁCIA PROFILU 49
9.4.2 PONUKA ŠTART A HLAVNÝ PANEL 50
9.4.3 OVLÁDACIE PANELY 51
9.4.4 PRACOVNÁ PLOCHA 52
9.4.5 PRIESKUMNÍK A SYSTÉM 52
9.4.6 APPLOCKER 53
9.5 KONFIGURÁCIA TENKÉHO KLIENTA 55
9.5.1 WRITE FILTER 56
9.5.2 HP EASY SHELL 56
9.5.3 KONFIGURÁCIA SYSTÉMU BIOS 57
9.5.4 DODATOČNÉ KONFIGURÁCIE 57
10 TESTOVANIE KONFIGURÁCIE 58
10.1 VYHODNOTENIE TESTOVANIA 61
ZÁVER 62
ZOZNAM POUŽITEJ LITERATÚRY 64
ZOZNAM POUŽITÝCH SKRATIEK 69
ZOZNAM OBRÁZKOV 71
ZOZNAM TABULIEK 72

ÚVOD

Bezpečnosť IT bola veľmi dlho podceňovanou témou. To, že server treba chrániť pred fyzickým prístupom a nie je vhodné ho umiestniť do firemnej kuchynky, kde sa denne vystrieda 99% zamestnancov, väčšina spoločností zistila už dávno. Fyzická ochrana je síce dôležitým prvkom, ale je to stále iba jeden z kamienkov v celej mozaike zabezpečenia. V dnešnej dobe, keď sa informačné systémy stali každodennou súčasťou nášho života, si postupne všetci začíname uvedomovať, aká je ochrana informácií dôležitá. Informácie sú dnes často najhodnotnejším aktívom. Ako ale ochrániť niečo, čo nemôžeme uchopiť? Server ako zariadenie vieme zobrať a presunúť do inej miestnosti, ale čo s informáciami, ktoré sú v ňom uložené? V tejto chvíli prichádzajú na scénu ďalšie formy zabezpečenia.
Operačné systémy v štandardnom nastavení ponúkajú iba základný stupeň zabezpečenia. Ak sa však použijú dodatočné technológie, ktoré sú bežne vo vnútropodnikovom prostredí dostupné, ako napr. Adresárové služby, Služby vzdialenej plochy, či komponenty zabezpečenia dát uložených na súborovom serveri, stupeň logického zabezpečenia sa okamžite rapídne zvýši.

V teoretickej časti mojej práce som sa snažil stručne popísať hlavné komponenty, pomocou ktorých dokáže aj menšia organizácia dosiahnuť zvýšenie existujúceho stupňa zabezpečenia. Postupne sú popísané jednotlivé komponenty Adresárových služieb, Služieb vzdialenej plochy, rôzne možnosti šifrovania dát, vybrané prvky infraštruktúry a výhody použitia konceptu tenkého klienta.

Praktická časť je následne zameraná na využitie spomínaných technológií a prostriedkov v reálnej praxi. Na základe zoznamu bezpečnostných požiadaviek fiktívnej výrobnej spoločnosti, sú postupne konfigurované jednotlivé služby a komponenty. Na konci kapitoly je potom popísaný funkčný test nasadeného riešenia, so stručným vyhodnotením s ohľadom na vstupné požiadaviek spoločnosti.

I. TEORETICKÁ ČASŤ

1 MICROSOFT WINDOWS SERVER 2012 R2

Spoločnosť Microsoft vydala svoj produkt Windows Server 2012 v auguste roku 2012. Táto verzia operačného systému je v komunite IT odborníkov považovaná za najväčší prelom od uvedenia Windows Server 2000. Pri návrhu bol kladený dôraz na dosiahnutie vysokej spätnej kompatibility zo staršími verziami. Za primárny cieľ si Microsoft vytýčil posun smerom k hlavným trendom v oblasti IT dnešných dní: orientácia na cloud, virtualizácia a zabezpečenie čo možno najvyššieho komfortu a mobility práce zákazníka (práca s mobilnými zariadeniami a vylepšovanie koncepcie BYOD[1] implementácií),

Windows Server 2012 prináša podstatne vylepšený zdrojový kód, ktorý je spoločný ako pre klientský operačný systém Windows 8, tak aj pre samotný Windows server. Preto nie je žiadnym prekvapením, že tieto dva na pohľad odlišné operačné systémy, obsahujú mnoho spoločných funkcií.

V októbri roku 2013 následne Microsoft vydáva balík kumulatívnych opráv, aktualizácií a vylepšení s označením „R2“.

1.1 Prehľad edícií a ich porovnanie

Windows Server 2012 R2 ponúka sedem rôznych edícií, z ktorých každá je orientovaná na iného cieľového zákazníka a odlišný typ použitia. Jednotlivé edície sa líšia licencovaním, hardvérovými obmedzeniami, aj zoznamom ponúkaných služieb.

V tabuľke nižšie, sú uvedené príklady hardvérových obmedzení a obmedzení súvisiacich s počtom pripájajúcich sa užívateľov, pre štyri najčastejšie používané edície Windows Server 2012 R2. Ďalšími tromi edíciami, potom sú: Microsoft Hyper-V Server 2012 R2, Windows Storage Server 2012 R2 Standard a Workgroup [1].

[1]BYOD (Bring Your Own Device) – koncept práce s vlastným „inteligentným“ zariadením ako napr. mobilný telefón, tablet, alebo osobný počítač v rámci firemnej siete a s firemnými dátami.

	Windows Server 2012 R2 Datacenter	Windows Server 2012 R2 Standard	Windows Server 2012 R2 Essentials	Windows Server 2012 R2 Foundation
Locks and Limits				
Maximum number of users	based on licenses	based on licenses	25	15
Maximum SMB Connections	16,777,216	16,777,216	16777216	30
Maximum RRAS Connections	unlimited	unlimited	50	50
Maximum IAS Connections	2,147,483,647	2,147,483,647	50	10
Maximum number of 64-bit sockets	64	64	2	1
Maximum RAM	4 TB	4 TB	64 GB	32 GB
Server can join a domain	Yes	Yes	For migration only	For migration only
DirectAccess	Yes	Yes	See documentation	Yes

Tab. 1: Porovnanie edícií Windows Server 2012 R2 [1].

1.2 Novinky vo Windows Server 2012 R2

Windows Server 2012 R2 prináša veľké množstvo vylepšení, ktoré je možné nájsť v každej jednej oblasti. V odstavcoch nižšie, sú popísané iba tie najzaujímavejšie, ktoré sa týkajú služieb Vzdialenej plochy (RDS).

1.2.1 RDS

„Er dvojka“ prináša zaujímavé vylepšenia a podporu v týchto oblastiach:

- Podpora Online systému odstránenia duplicitných dát (Online Data Deduplication) – funkciu odstránenia duplicitných dát, predstavenú vo Windows Server 2012, môže správca využiť aj v spojení so službami vzdialenej plochy. Ak sú užívateľské profily uložené ako virtuálne disky[2] na súborovom serveri, dá sa týmto spôsobom radikálne znížiť kapacita potrebná na uloženie týchto údajov. Zároveň služba ukladá do svojej rýchlej medzipamäte dáta, ku ktorým sa pristupuje najčastejšie a tým značne urýchľuje proces ich opätovného načítania v prípade potreby [3].
- Tieňovanie užívateľských relácií (Session Shadowing) – umožňuje vzdialene kontrolovať, alebo riadiť aktívne relácie iného užívateľa pripojeného k hostiteľovi vzdialenej plochy. Bola pridaná podpora priamo do príkazu „mstsc.exe“ [3].

[2]Virtuálny disk (VHD) – *„je súbor uložený na súborovom systéme, ktorého vnútorná štruktúra je rovnaká ako štruktúra fyzického pevného disku“ [2].*

- Rýchle obnovenie pripojenia klientov vzdialenej plochy (Quick Reconnect for Remote Desktop Clients) – proces opätovného pripojenia užívateľa k službám vzdialenej pracovnej plochy bol optimalizovaný na dosiahnutie vyššieho výkonu. Zároveň bol systém vo Windows server 2012 R2 prepracovaný a doplnený o podrobnejšie informačné hlášky a užívateľsky príjemnejšie rozhranie [3].
- Vylepšená kompresia a využitie šírky pásma (Improved Compression and Bandwidth Usage) – nasadenie vylepšených kompresných algoritmov môže viesť až k 50% úspore pri prenose dát oproti Windows Server 2012 a tým k efektívnejšiemu využitiu prenosového pásma [3].
- Dynamické spracovanie zobrazenia (Dynamic Display Handling) – vo Windows 8.1 a Windows Server 2012 R2 bola pridaná podpora, ktorá zaisťuje, že zmeny v zobrazovaní na klientskej stanici, ako sú pridanie a odobratie zobrazovacieho zariadenia, alebo rotácia zariadenia, sa automaticky prejavia aj v klientovej vzdialenej relácií [3].
- Podpora DirectX 11.1 (RemoteFX Virtualized GPU Supports DX11.1) – podpora DirectX rozhrania na systémoch, ktoré majú kompatibilnú grafickú kartu. Graficky náročne aplikácie, ktoré dokážu využiť túto funkcionalitu, teraz môžu byť virtualizované a prevádzkované na Windows 8, alebo Windows Server 2012 R2 [3].
- Zmeny v nastavení pamäte grafického adaptéra (Video RAM Changes) – pridanie systémovej pamäte virtualizačnému serveru, teraz umožňuje dynamické navýšenie pamäte pre grafický adaptér virtuálnych počítačov. Týmto sa môže zlepšiť výkon virtualizovaných aplikácií [3].
- Režim RestrictedAdmin pre vzdialenú plochu (RestrictedAdmin Mode Remote Desktop) – *„pri pripojení pomocou tohoto režimu, neodosiela klient vzdialenej plochy prihlasovacie údaje hostiteľskému serveru. Pri použití tohto režimu s prihlasovacími údajmi správcu, sa klient vzdialenej plochy pokúsi pripojiť interaktívne, bez odoslania prihlasovacích údajov hostiteľovi. Keď hostiteľ overí, že užívateľský účet, ktorý sa k nemu pripája, má práva správcu, a podporuje daný režim, je pripojenie úspešné. V opačnom prípade je pripojenie neúspešné. V tomto režime sa vzdialeným počítačom v žiadnom okamihu neposielajú prihlasovacie údaje ako jednoduchý text, ani v nejakej inej opakovateľne použiteľnej forme“ [3].*

1.3 Licencovanie

Licencovanie pre edície Datacenter a Standard sú z pohľadu hardvéru totožné. Jedna licencia pokrýva server s dvoma fyzickými procesormi. Zároveň obidve edície obsahujú rovnakú sadu aplikácií a rolí. Základný rozdiel spočíva v počte virtuálnych serverov, ktoré je možné v rámci danej licencie nainštalovať. V prípade Standard licencie, sú to dva virtuálne servery, v prípade Datacenter licencie, je počet obmedzený iba výkonom virtualizačného servera.

Licensing examples	Datacenter licenses required	Standard licenses required
One 1-processor, non-virtualized server	1	1
One 4-processor, non-virtualized server	2	2
One 2-processor server with three virtual OSEs	1	2
One 2-processor server with 12 virtual OSEs	1	6

Tab. 2: Potrebné množstvo licencií pre jednotlivé nasadenia [5].

1.4 Hardvérové požiadavky

Komponent	**Minimálne Požiadavky**
Procesor	1.4 GHz (64-bit procesor) alebo rýchlejší
Operačná Pamäť	512 MB
	800 MB v prípade virtualizácie
Pevný Disk	32GB
Sieťový Adaptér	Sieťová Karta (10/100/1000baseT)
Dodatočné Požiadavky (Inštalácia OS)	DVD-ROM, USB kľúč, ...

Tab. 3: Minimálne hardvérové požiadavky [6].

2 ACTIVE DIRECTORY DOMAIN SERVICES (AD DS)

Prvý krát sa služba Active Directory (AD) objavila v systéme Windows Server 2000 v roku 1999 a odvtedy prešla mnohými vylepšeniami. S príchodom Windows Server 2008, bola služba premenovaná na Active Directory Domain Services, čo môžeme voľne preložiť aj ako „Adresárová služba“.

AD DS je v súčasnosti rola, nainštalovaná na serveri plniacom funkciu doménového radiča. Táto služba je považovaná za kľúčový komponent v riadení prístupov a identít v korporátnych sieťach, založených na Microsoft technológiách.

„*Active Directory je centrálnym úložiskom pre konfiguračné informácie, požiadavky na overovanie a informácie o všetkých objektoch uložených v doménovej štruktúre*“ *[7].*

Služba poskytuje prostriedky pre centralizovanú správu a konfiguráciu sieťových zdrojov, identít a vzťahov, v rámci firemnej siete. Zároveň ponúka nástroje, ktoré zjednodušujú správu používateľov, počítačov a iných objektov uložených v AD databáze. Umožňuje povoliť prístup k sieťovým prostriedkom pomocou jednotného prihlasovania (SSO) a zvyšuje ochranu a zabezpečenie uložených informácií [4, 7].

Štruktúru AD DS môžeme rozdeliť na Fyzickú a Logickú.

2.1 Fyzická Štruktúra

Pod fyzickou štruktúrou si môžeme predstaviť servery, či sieťovú infraštruktúru, potrebnú pre správnu funkčnosť adresárových služieb.

2.1.1 Doménové radiče (Domain Controllers)

Doménový radič (alebo Doménový kontroler) je fyzický, alebo virtuálny server, ktorý má nainštalovanú rolu AD DS a na súborovom systéme má fyzicky umiestnený súbor – AD databázu. Keďže databáza okrem iného obsahuje aj informácie o všetkých účtoch v doméne, je **doménový radič kritickým komponentom** infraštruktúry. Je preto nevyhnutné zabezpečiť, aby nedošlo k jeho kompromitácii a to ako po stránke fyzickej, tak aj logickej.

2.1.2 Active Directory Lokalita (Active Directory Site)

Lokalita reprezentuje fyzickú štruktúru siete danej organizácie. Väčšinou združuje skupinu serverov, prepojených rýchlou a spoľahlivou sieťovou linkou. Obecne môžeme povedať, že jej primárnou úlohou je vytvoriť „hranicu“ pre replikáciu dát, medzi radičmi domény. Správne nastavenie lokalít, je preto dôležité pre zabezpečeniu optimálnej komunikácie medzi jednotlivými doménovými radičmi a má rozhodujúci vplyv na zaťaženie siete.

2.1.3 Active Directory particie (Active Directory Partitions)

AD databáza je vnútorne členená na jednotlivé partície. Každá z partícii obsahuje špecifické dáta a má svoj vlastný replikačný rozsah[3] (Replication Scope).
Jednotlivé partície:

- Doménová partícia (Domain Partition) - je replikovaná iba medzi doménovými radičmi v rámci domény. Nachádzajú sa tu napr. užívateľské a počítačové účty, skupiny, a iné objekty vytvorené v danej doméne [8].
- Konfiguračná partícia (Configuration Partition) – obsahuje konfiguračné nastavenia pre celý les. Vykonané zmeny sa preto replikujú na všetky doménové kontrolery v lese [8].
- Schéma (Schema Partition) – Microsoft Active Directory schéma, sa dá obecne nazvať šablónou. Obsahuje definície každého jedného objektu, tried atribútov[4] aj samotných atribútov. Na základe týchto definícií, je následne možné v AD vytvárať objekty. Tak, ako konfiguračná partícia, aj schéma je replikovaná na všetky doménové radiče v lese [8].
- Aplikačná partícia (Application Partition) – je partícia využívaná pre špecifické aplikácie, alebo účely. Je voliteľná, a preto sa nemusí nachádzať na každom doménovom kontrolery. Administrátor môže definovať, na ktoré doménové radiče sa táto partícia bude replikovať [8].

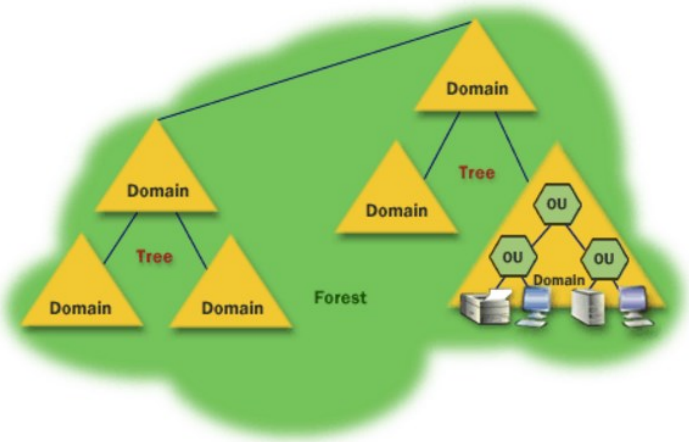
[3] Replikačný rozsah v tomto prípade znamená, na ktoré konkrétne doménové radiče sa bude partícia replikovať.

[4] Atribút je hodnota, alebo informácia, ktorá charakterizuje daný objekt. Každý atribút môže obsahovať jednu, alebo viac hodnôt, napr. meno, priezvisko, telefónne číslo, atď. [10].

- Globálny katalóg (Global Catalog) – nie je partíciou v pravom slova zmysle. Je však dôležitý pre určité aplikácie a scenáre, ako napríklad MS Exchange mailový systém. Obsahuje vybrané atribúty každého objektu, z každej domény v lese [4, 9].

2.2 Logická Štruktúra

Logická štruktúra Adresárovej služby je z pohľadu administrátora nezávislá na fyzickej štruktúre. Pre spoľahlivé nasadenie je však odporúčané, aby boli nastavenia optimalizované, s ohľadom na fyzickú infraštruktúru spoločnosti [11].



Obr. 1: Logická štruktúra Adresárovej služby (doména, strom a les) [12].

2.2.1 Doména (Domain)

Doména je logickým zoskupením objektov (ako napr. počítače, užívatelia a tlačiarne) uložených v jednej AD databáze, ktoré zdieľajú spoločné bezpečnostné politiky [4, 13].
Doménu zároveň môžeme definovať ako:

- *„Základnú jednotku replikácie dát*
- *Autentifikačnú a Autorizačnú hranicu*
- *Jeden z kontajnerov v rámci doménového stromu*
- *Jednotka vzťahu dôveryhodnosti*
- *Jednotka pre aplikáciu politík“ [13].*

Každá doména, má definovanú skupinu Doménových Administrátorov, ktorej členovia majú plné práva na všetky objekty v danej doméne. Tieto oprávnenia, sú platné iba v rámci ich domény a nepremietajú sa automaticky do iných domén v strome, alebo lese.

2.2.2 Strom (Tree)

Doménový strom slúži ako logické zoskupenie jednotlivých domén a reprezentuje unikátny menný priestor systému doménových mien (DNS namespace) [4, 13].

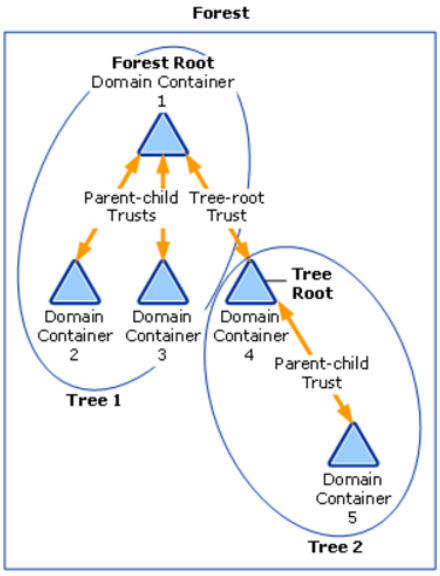
2.2.3 Les (Forest)

Funkciou doménového lesa je zoskupovať jednotlivé doménové stromy, ktoré majú medzi sebou automaticky nadviazaný vzťah dôveryhodnosti (Trust[5]) [4, 13].
Les je zároveň:

- *„Kolekcia doménových kontajnerov, ktoré dôverujú jeden druhému*
- *Jednotka replikácie*
- *Bezpečnostná hranica**
- *Jednotka delegácie“ [13].*

*Pretože je les bezpečnostnou hranicou a jeden les štandardne nemá nadviazaný vzťah dôveryhodnosti s iným lesom, ani užívatelia nemajú povolený prístup z jedného lesa do iného [13].

[5] *„Trust umožňuje, aby užívatelia v jednej doméne, boli radičom domény overení v inej doméne“ [14].*



Obr. 2: Doména, strom, les a vzťahy dôvery [13].

2.2.4 Rola hlavného operačného servera (FSMO)

Nie všetky konfiguračné zmeny v rámci Adresárových služieb je vhodné vykonávať štandardným spôsobom, čo znamená na ľubovoľnom doménovom radiči. Pre definované kritické operácie bolo preto v prostredí Microsoft Adresárových služieb definovaných päť špecifických rolí (tzv. FSMO role). Tieto FSMO role, sú priradené jednému, alebo rozdelené medzi viacero doménových radičov [15].

FSMO role uvedené nižšie, sa podľa rozsahu ich použitia delia na dva základné typy:

- Role platné pre celý les - hlavný server schém a hlavný server názvov domén [16].
- Role platné pre celú doménu - hlavný server infraštruktúry, hlavný server relatívnych ID a emulátor primárneho radiča domény [16].

Stručný popis jednotlivých FSMO rolí:

- Hlavný server schém (Schema Master) – *„radič domény predstavujúci hlavný server schém, riadi všetky aktualizácie a úpravy schémy. Ak chcete aktualizovať schému doménovej štruktúry, musíte mať prístup k hlavnému serveru schém. V celom lese sa môže nachádzať iba jeden takýto server“ [16].*
- Hlavný server názvov domén (Domain Naming Master) – *„riadi pridávanie alebo odstraňovanie domén v doménovej štruktúre. V celom lese sa môže nachádzať iba jeden hlavný server názvov domén“ [16].*

- Hlavný server infraštruktúry (Infrastructure Master) – *„je zodpovedný za aktualizáciu odkazov jednotlivých objektov vo svojej doméne na objekty v ostatných doménach. V ľubovoľný okamih môže v danej doméne existovať len jeden radič domény, fungujúci ako hlavný server infraštruktúry" [16].*
- Emulátor primárneho radiča domény (PDC Emulator) – plní v doméne dôležité bezpečnostné úlohy, ako sú:
    - Zmeny hesiel vykonané na iných doménových radičoch, sú primárne replikované na PDC
    - Proces uzamykania účtov je spracovávaný na PDC
    - Ak sa užívateľ nemôže prihlásiť z dôvodu zadania zlého hesla, miestny doménový radič prepošle požiadavku na posúdenie PDC – tento má vždy najaktuálnejšie informácie o aktuálnych heslách [17].

  Zároveň je PDC hlavný prehliadačom domény a plní rolu spoľahlivého zdroja času, pre všetky servery a klientské stanice danej domény. Tak ako bolo spomenuté pri ostatných roliach, aj táto musí byť v danej doméne jedinečná [16].
- Hlavný server relatívnych ID (RID Master) – je zodpovedný za spravovanie rozsahu RID identifikátorov (tzv. RID pool)[6]. Na požiadanie prideľuje doménovým radičom vždy unikátny rozsah číselných hodnôt, ktoré neskôr využijú pri vytváraní doménových objektov. V každej doméne môže v jednej chvíli existovať iba jeden server plniaci túto funkciu [18].

[6] Každý doménový objekt, ktorému vieme priradiť bezpečnostné oprávnenia (skupina, užívateľ, počítač,...) vytvorený v doméne, musí byť unikátny a jednoznačne identifikovateľný. Na toto slúži tzv. bezpečnostný identifikátor (SID). Aby bol doménový radič schopný zabezpečiť unikátnosť, tohto identifikátora, je SID objektu zložený z dvoch častí. Prvá časť, rovnaká pre všetky objekty danej domény – bezpečnostný identifikátor domény (Domain SID). Druhá časť, unikátne číslo z rozsahu (RID pool), ktorý bol exkluzívne tomuto doménovému radiču pridelený hlavným serverom relatívnych ID [4, 18].

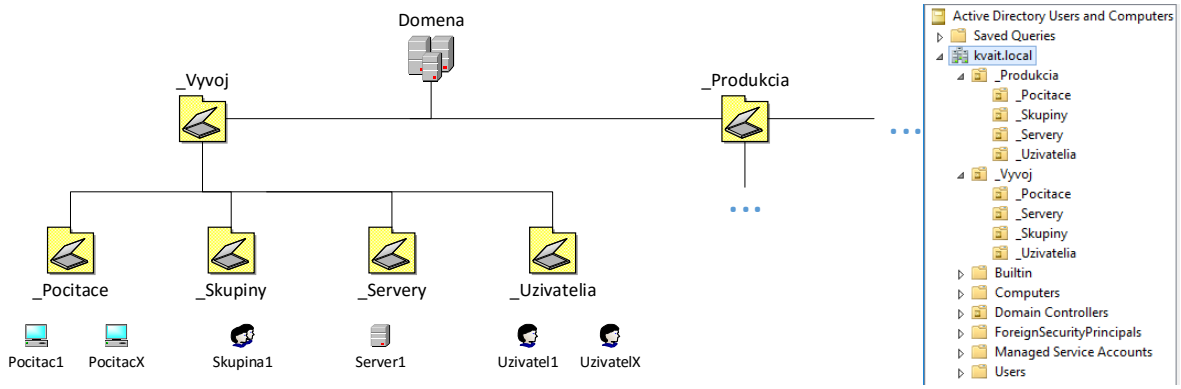
2.2.5 Organizačné jednotky (OU)

Adresárová služba umožňuje správcom vytvárať hierarchickú doménovú štruktúru, ktorá spĺňa potreby ich organizácie. Organizačné jednotky sú objekty, ktoré umožňujú tento cieľ dosiahnuť. Slúžia na združovanie jednotlivých objektov, ako sú skupiny, užívatelia, počítače, zdieľané prostriedky, či tlačiarne. Organizačnú jednotku si môžeme predstaviť ako adresár na súborovom systéme, kde máme podľa nejakého kľúča, alebo spoločnej vlastnosti uložené dokumenty rôzneho typu [19].

Jednotlivé organizačné jednotky môžeme vnárať jednu do druhej a vytvoriť tak požadovanú hierarchiu, odzrkadľujúcu logickú štruktúru organizácie. Štruktúra organizačných jednotiek v rámci jednotlivých domén je na sebe nezávislá, čo umožňuje správcom domén maximálnu flexibilitu [19].

Aj keď ako bolo spomenuté vyššie, každý administrátor si môže vytvoriť svoju vlastnú hierarchickú štruktúru organizačných jednotiek, aj v tomto smere existuje niekoľko najčastejšie používaných modelov:

- Geografický model – štruktúra odzrkadľujúca regionálne rozdelenie organizácie [20].
- Plochý (Shallow) model – plochá štruktúra s minimálnym počtom nadradených organizačných jednotiek [20].
- Rozdelenie na základe typu uloženého objektov (Type – Based model) [20].
- Kombinovaný model – je kombináciou vyššie uvedených modelov.



Obr. 3: Model kombinovanej hierarchie organizačných jednotiek, vlastný zdroj.

Organizačná jednotka je najmenšou jednotkou, na ktorú je možné priraďovať doménové skupinové politiky. Zároveň, čo je dôležité z pohľadu bezpečnosti, je aj základným prvkom, na ktorý vieme delegovať rôzne typy oprávnení. Vybranej skupine správcov, zodpovedným za podporu koncových staníc, nie je napríklad nevyhnutné prideľovať maximálne oprávnenia v rámci celej domény. Vieme im delegovať iba vybrané činnosti, ktoré budú schopní vykonávať na objektoch umiestnených v konkrétnej organizačnej jednotke. Napr.: povolíme reset hesla, zakážeme zmazanie účtu.

2.2.6 Skupiny

Skupiny sú jedným z najdôležitejších komponentov doménovej infraštruktúry, pre správu prístupových oprávnení. Pomocou združovania jednotlivých účtov (či už užívateľských, počítačových, alebo iných) do bezpečnostných skupín, sa zjednodušuje a sprehľadňuje proces prideľovania a riadenia oprávnení k jednotlivým prostriedkom.

2.2.6.1 Typy skupín

V AD sa využívajú dva základné typy skupín

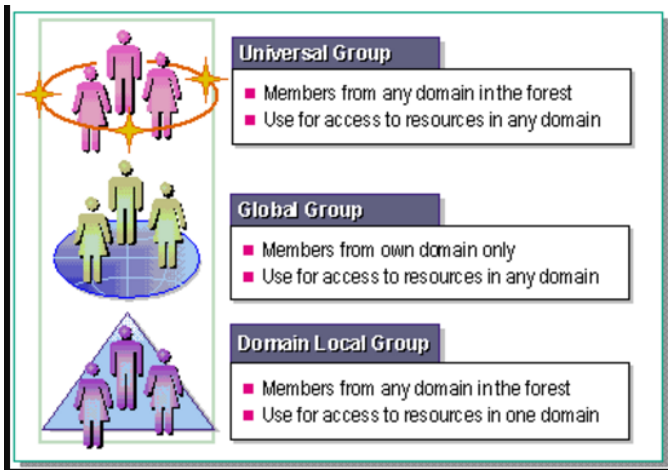
- Distribučné skupiny (Distribution Groups) – tento typ skupín využívajú mailové aplikácie ako distribučný zoznam užívateľov [21].
- Bezpečnostné skupiny (Security Groups) – umožňujú riadiť prístup k prostriedkom v doméne [21].

2.2.6.2 Rozsah skupín

Jednotlivé skupiny sú charakterizované rozsahom, ktorý určuje, do akej miery sa dá skupina v doménovej hierarchii použiť. Každá zo skupín má svoje unikátne vlastnosti a obmedzenia, čo sa týka objektov, ktoré do nej môžeme vložiť a vnárania iných skupín. Rozlišujeme tri základné typy rozsahov skupín:

- Miestne, alebo aj lokálne doménové skupiny (Local Domain Group) – slúžia iba na definovanie prístupu k prostriedkom v doméne, kde existuje daná miestna doménová skupina [21].

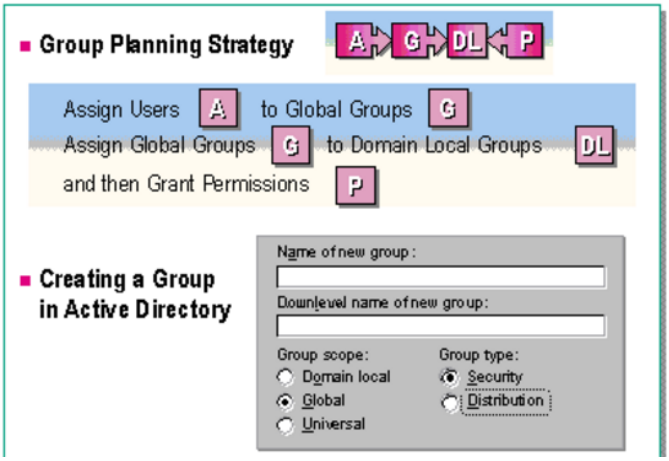
- Globálne skupiny (Global Groups) – sú primárne používané na zoskupovanie doménových objektov (užívateľov, iných globálnych skupín a počítačov), na základe ich spoločných vlastností (napr. rola v danej organizácii) [21].
- Univerzálne skupiny (Universal Groups) – *„členom tejto skupiny, je možné priradiť oprávnenia v ľubovoľnej doméne v doménovej štruktúre, alebo jej vetve. Skupiny sa používajú ku konsolidácií skupín presahujúcich hranice domény“ [21].*



Obr. 4: Rozsah skupín [22].

2.2.6.3 Odporúčaný model použitia

Diagram nižšie ukazuje odporúčaný model použitia jednotlivých skupín – stratégia **AGDLP**. Užívatelia sú umiestnený do globálnej skupiny, globálna skupina do lokálnej doménovej skupiny a doménovým lokálnym skupinám sú pridelené požadované oprávnenia, ku jednotlivým zdrojom [22].



Obr. 5: Model použitia skupín – AGDLP [22].

V prípade použitia univerzálnych skupín, by sa potom tento model rozšíril na **AGUDLP** – užívateľ je členom globálnej skupiny, táto je následne vložená do univerzálnej a univerzálna do miestnej doménovej skupiny, ktorej pridelíme požadované oprávnenia.

2.2.7 Ďalšie dôležité objekty

Každý objekt umiestnený v AD databáze, je na základe schémy tvorený skupinou atribútov. Zároveň, je každý jeden objekt jednoznačne definovaný unikátnym identifikátorom GUID (Globally Unique Identifier). Tento identifikátor sa počas „života" daného objektu nemení a nemá na neho vplyv ani presun, či premenovanie objektu [4, 23].

2.2.7.1 Užívateľ (User)

Systém Microsoft Windows pozná dva základné typy užívateľských účtov.

- Lokálny užívateľ – užívateľ na konkrétnej pracovnej stanici, alebo serveri. Lokálny užívatelia existujú rovnako v doménovom aj ne-doménovom prostredí. Jedinou výnimkou je server, plniaci rolu doménového radiča. Tento server neobsahuje lokálnych užívateľov – obsahuje iba špeciálny typ lokálneho užívateľa, pre prípad nefunkčnosti adresárových služieb.

  S lokálnymi užívateľmi sú úzko späté lokálne skupiny. Tieto sú automaticky vytvorené pri inštalácii operačného systému. Tak, ako pri lokálnych užívateľoch aj pri skupinách platí, že doménový radič tieto skupiny neobsahuje.
- Doménový užívateľský účet – užívateľský účet vytvorený v AD, ktorý umožňuje jednotné prihlásenie v rámci domény. Štandardne obsahuje informácie, ako sú užívateľské meno, heslo a členstvo v doménových bezpečnostných skupinách [23].

2.2.7.2 Počítač (Computer)

Počítačový objekt reprezentuje pracovnú stanicu, server, alebo iné zariadenie, pripojené do siete. Tento objekt je dôležitý pre autentifikáciu a autorizáciu daného zariadenia v AD infraštruktúre. Počítačový účet sa vytvorí alebo automaticky pri pridaní počítača do domény, alebo ho administrátor môže vytvoriť manuálne [24].

2.2.7.3 Zdieľaný priečinok (Share)

Reprezentuje priečinok, vyzdieľaný na serveri v sieti. Vďaka tomuto objektu, vedia užívatelia vyhľadávať zdieľané adresáre a pristupovať tak k firemným dátam.

2.2.7.4 Tlačiareň (Printer)

Prostredníctvom objektu tlačiarne je možné vytvárať a následne spravovať tlačiarne, zapojené v TCP/IP sieti, alebo pripojené k serverom v korporátnej sieti [23].

2.2.8 Skupinové politiky (Group Policy)

Skupinové politiky (GPO), takisto označované ako Zásady skupiny, predstavujú sadu pravidiel a nastavení, ktoré umožňujú centralizovanú správu a konfiguráciu počítačov, aplikácií, ako aj nastavení operačného systému a samotných užívateľov pracujúcich v prostredí Microsoft AD. Pre mnoho organizácii sa preto skupinové politiky stali jedným z kľúčových prvkov na uľahčenie dennej administrácie.

V zásade rozoznávame dva typy skupinových politík. Prvou skupinou sú politiky priamo na klientskej stanici. Tieto sa aplikujú vždy a existujú aj vtedy, ak klient nie je členom domény. Druhým typom sú doménové skupinové politiky, ktoré sa na systém aj samotného užívateľa aplikujú iba vtedy, ak je členom domény. Čo je dôležité poznamenať je to, že doménové skupinové politiky sa štandardne priraďujú na lokalitu (Site), doménu (Domain) alebo organizačnú jednotku (OU). Podľa toho, kde sa v doménovej štruktúre objekt nachádza, podľa toho sa na neho aplikujú priradené politiky [25, 44].

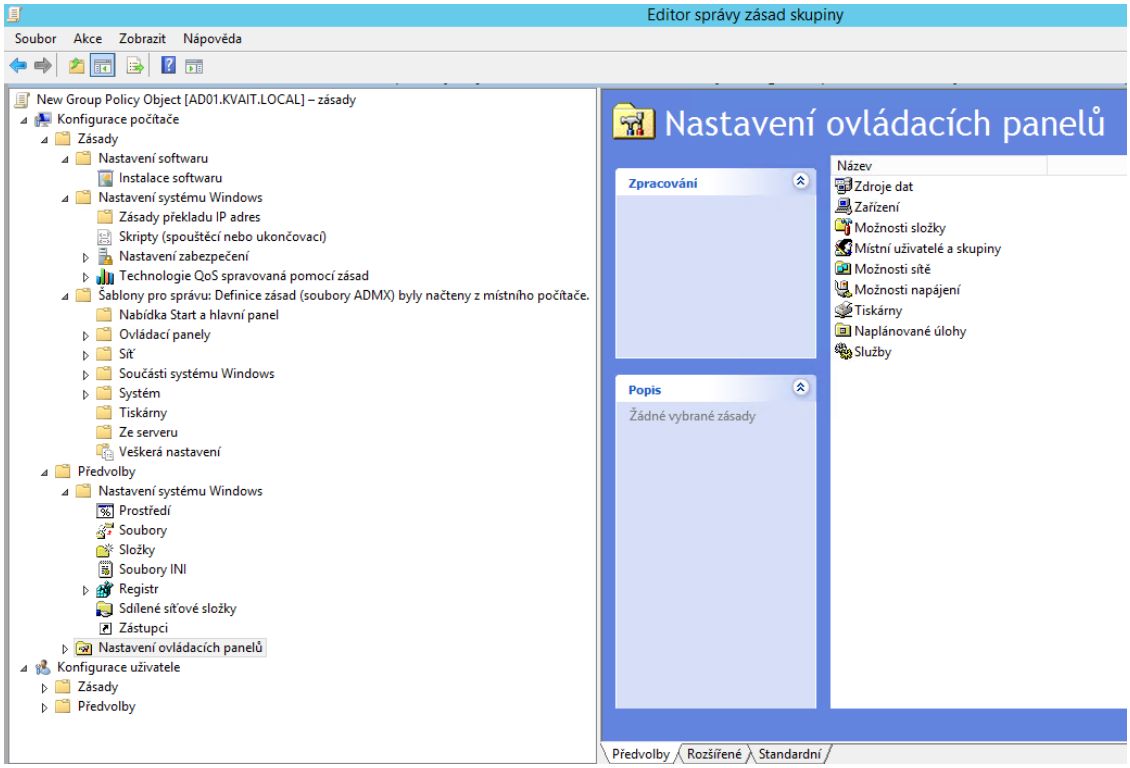
Politiku nie je možné priradiť na bezpečnostnú skupinu (Security Group).
Skupinové politiky obsahujú tisíce rôznych nastavení, rozdelených do niekoľkých základných skupín.

- Skupina nastavení – Zásady (Policies) – primárne slúži na riadenie konfigurácie operačného systému a jeho jednotlivých komponentov. Obsahuje mnoho nastavení, ktoré sa aplikujú na počítač aj na užívateľa. Skupina sa delí na tri základné triedy:
    - Nastavenie softvéru (Software Settings) – inštalácia a aktualizácia softvéru.

  - Nastavenia Systému Windows (Windows Settings) – prihlasovacie a štartovacie skripty, bezpečnostné nastavenia, ako napr. konfigurácia systémových služieb, parametrov logovania, firewall nastavení.
  - Šablóny pre správu (Administrative Templates) – obsahuje konfiguračné položky, určené na modifikáciu pracovnej plochy, zdieľaných priečinkov, siete a iných komponentov operačného systému. Šablóny pre správu môžu byť v prípade potreby rozšírené o ďalšie konfiguračné položky, napr. pre správu aplikácií balíka Microsoft Office [23].
- Skupina nastavení – Predvoľby (Preferences) – umožňujú nastavovať v podstate všetko, čo je konfigurovateľné záznamom v registry databáze na klientskom systéme. Skupina obsahuje dve základné triedy:
  - Windows nastavenia (Windows Settings) – nastavenia ako mapovanie diskov, vytváranie odkazov na pracovnej ploche, či vytváranie záznamov v registry databáze.
  - Nastavenie ovládacieho panelu (Control Panel Settings) – regionálne nastavenia, nastavenia Internet Explorera, prispôsobenie štart ponuky a iné.

Prvú skupinu (Zásady), je možné označiť aj ako „tvrdé politiky“. Ich nastavenia sú vynucované a užívateľ nemá možnosť ich meniť. Na rozdiel od prvej skupiny, Predvoľby vynucované nie sú [26].

Na konfiguráciu jednotlivých nastavení skupinových politík, slúži Editor správy zásad skupiny (Group Policy Management Editor). Správca môže editor spustiť priamo z doménového radiča, alebo zo svojej klientskej stanice, po doinštalovaní balíka nástrojov pre vzdialenú administráciu serverov (RSAT).



Obr. 6: Editor správy zásad skupiny (Group Policy Management Editor), vlastný zdroj.

2.2.8.1 Nastavenia aplikované na Počítač (Computer Configuration)

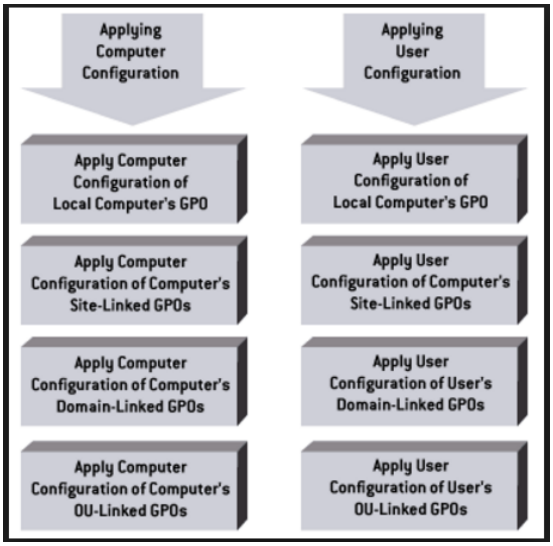
Nastavenia, ktoré administrátor nakonfiguruje v tejto vetve, sa aplikujú na počítačové objekty, ktoré sa nachádzajú v organizačnej jednotke, na ktorú je daná politika priradená. Modifikujú nastavenia daného počítača a aplikujú sa pri jeho štarte. Preto nezáleží na tom, aký užívateľ sa na počítač či server hlási [27].

2.2.8.2 Nastavenia aplikované na užívateľa (User Configuration)

Ako už názov napovedá, tieto nastavenia sa aplikujú na konkrétneho užívateľa, alebo skupinu užívateľov. Nastavenia s používateľom „cestujú“, čo znamená, že na akýkoľvek počítač sa prihlási, skupinová politika, ktorú mu administrátor priradil, sa bude pri prihlásení užívateľa aplikovať [27].

2.2.8.3 Spôsob Aplikovania politík

Pod spôsobom, alebo poradím aplikovania politík rozumieme postupnosť, s akou sa na daný objekt politiky aplikujú. V každej organizácii je viac ako pravdepodobné, že na objekt sa bude aplikovať viac ako len jedna skupinová politika. Je preto dôležité vedieť, ktoré z nastavení sa v prípade konfliktu finálne aplikujú (jedna politika nastaví kľúč A v registroch na hodnotu 1, druhá politika nastaví ten istý kľúč na hodnotu 2). Jednoduchým pravidlom, ktoré si treba zapamätať je, že posledná politika ktorá sa aplikuje, prepisuje všetky kolízne nastavenia aplikované predošlými politikami. Zároveň politika, ktorá je ku klientovi najbližšie z hľadiska doménovej štruktúry, je aplikovaná ako posledná [25, 44].
Poradie aplikovania politík je teda nasledovné:



Obr. 7: Spôsob aplikovania politík [28].

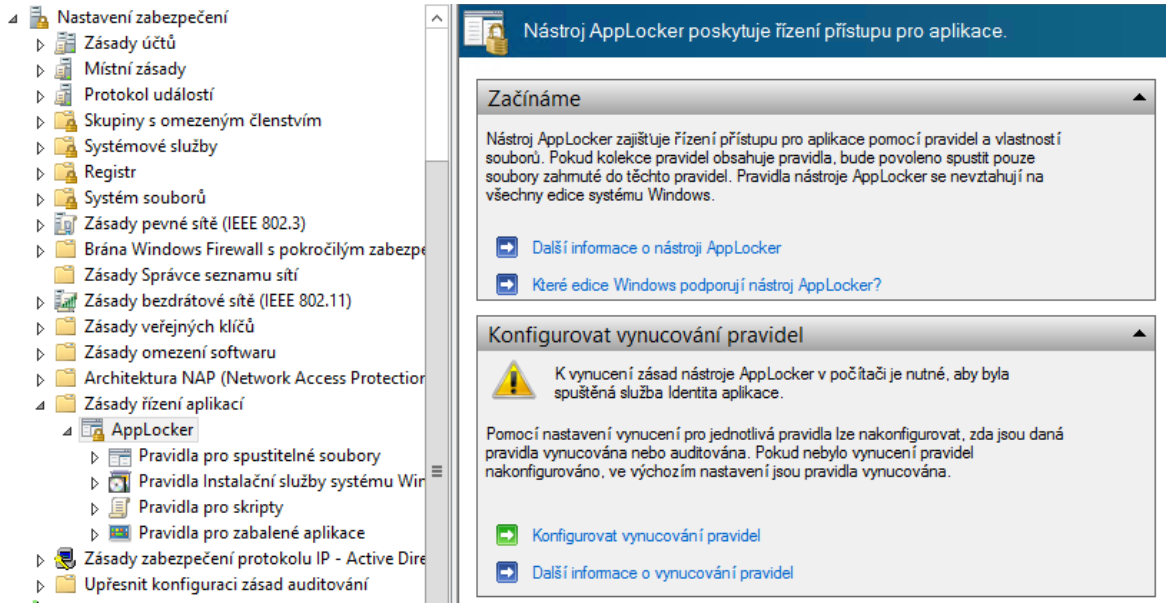
Prvá sa aplikuje miestna (Local) politika, následne politika danej lokality (Site), po nej doménová (Domain) a ako posledná, sa aplikuje politika priradená na organizačnú jednotku (OU), kde sa samotný objekt nachádza.

2.2.8.4 Applocker

Applocker poskytuje riadenie prístupu pre aplikácie. Je jedným z bezpečnostných nastavení doménových skupinových politík. Nastavenia sa aplikujú na počítač, čo znamená, že nezáleží na tom, aký užívateľ sa na daný server alebo pracovnú stanicu prihlási.

Applocker umožňuje správcom povoliť, alebo zakázať jednotlivým užívateľom, alebo skupine užívateľov prístup k definovaným súborom, aplikáciám, alebo skriptom. Definuje pravidlá pre štyri základné kategórie: spustiteľné súbory, inštalačná služba systému Windows, skripty a zabalené aplikácie. Správca je schopný:

- Definovať pravidlá na základe umiestnenia, otlačku súboru (Hash) a parametrov vydavateľa (Publisher) súboru, ako sú digitálny podpis, vydavateľ aplikácie, názov a verzia súboru. Správca môže napríklad vytvoriť pravidlo, že užívatelia bezpečnostnej skupiny „A“ majú zakázané spúšťať produkty spoločnosti Adobe, okrem Adobe Reader verzie 9.
- Priradiť pravidlo na vybranú bezpečnostnú skupinu, alebo jednotlivých užívateľov.
- Vytvorenie výnimky z pravidiel – je možné napríklad vytvoriť pravidlo, ktoré povolí spustenie všetkých Windows procesov, okrem príkazového riadku (cmd.exe).
- Nasadiť politiku v audit režime – nastavenia nie sú vynucované, čo znamená, že užívateľ nie je politikou nijako obmedzovaný. Spúšťanie aplikácií je však zaznamenávané do protokolu udalostí, kde administrátor vidí, aký vplyv budú mať jeho nastavenia na daného užívateľa, alebo skupinu užívateľov.
- Export a import Applocker nastavení – administrátor je schopný exportovať svoje nastavenia do XML súboru, alebo naopak importovať uložené nastavenia [29].



Obr. 8: Applocker skupinová politika, vlastný zdroj.

2.3 Ďalšie možnosti zabezpečenia

Adresárová služba ponúka prostredníctvom skupinových politík obrovské množstvo nastavení, kombináciou ktorých môže každá organizácia efektívne zvýšiť úroveň bezpečnosti svojej IT infraštruktúry. Aj keď je pravda, že nie každá jedna vlastnosť operačného systému sa dá nastaviť priamo cez editor správy zásad skupín, vždy existuje možnosť, ako dosiahnuť požadovanú konfiguráciu (či už skriptom, alebo vzdialenou modifikáciou databázy registry, prípadne zmenou konfiguračného súboru uloženého na súborovom systéme). V odstavcoch nižšie je preto uvedených niekoľko bodov a konkrétnych nastavení, ktoré sú z pohľadu logickej bezpečnosti kľúčové. Pre lepšiu orientáciu boli rozdelené do niekoľkých kategórií.

2.3.1 Delegovanie právomocí

Jednotliví správcovia majú v organizácií určitú náplň svojej práce. Len zriedkavo je naozaj nevyhnutné, aby mal každý správca plné oprávnenia na každý jeden objekt v AD.

Delegovanie právomocí na jednotlivé organizačné jednotky – na základe AD bezpečnostných skupín, je možné prideliť správcom zodpovedným za určité administratívne činnosti iba oprávnenia nevyhnutne potrebné pre výkon ich práce. Právomoci je možné delegovať až na úrovni atribútov jednotlivých objektov.

„Bežné úlohy, pre ktoré je možné delegovať oprávnenia:

- *Vytvorenie, odstránenie a správa užívateľských účtov*
- *Obnovenie užívateľských hesiel, vynútenie zmeny hesla pri ďalšom prihlásení*
- *Čítanie všetkých informácií o užívateľovi*
- *Pridanie počítača do domény“ [30].*

2.3.2 Užívateľské heslá

Sila a parametre uzamykania užívateľských účtov, sú jedným z najkritickejších parametrov. Pokiaľ o heslá počítačových účtov, sa stará systém sám, heslá k užívateľským účtom sú často najväčšou slabinou zabezpečenia IT infraštruktúry. Preto je veľmi dôležité zaviesť rozumnú firemnú politiku hesiel. V rámci adresárových služieb k tomu slúži Predvolená doménová politika (Default Domain Policy), ktorá umožňuje definovať:

- Zásady užívateľských hesiel – zložitosť, dĺžka, doba platnosti, či história zapamätaných hesiel.
- Zásady uzamknutia účtov – doba, prahové hodnoty a parametre pre vynulovanie čítača uzamknutia.

2.3.3 Auditing a Protokoly udalostí

Auditovanie zmien konfigurácií, či iných zásahov a ich zaznamenávanie, je nevyhnutným predpokladom k úspešnej diagnostike a následnému riešeniu problémov.

- Auditovanie – okrem základných nastavení, ktoré sú prednastavené pri inštalácii, má správca k dispozícií ďalších 53 rôznych položiek pokročilého auditu, ktoré umožňujú sledovať každý jeden element adresárových služieb. Jednotlivé nastavenia sú rozdelené do niekoľkých hlavných kategórií: Prihlásenie k účtu, Správa účtov, Podrobné sledovanie, Prístup k adresárovej službe, Prihlásenie a odhlásenie, Prístup k objektu, Zmeny zásady, Oprávnenosť použitia, Systém a Globálne auditovanie prístupu k objektom [31].
- Protokoly udalostí – umožňujú definovať parametre aplikačného a systémového protokolu udalostí a protokolu zabezpečenia.

2.3.4 Zabezpečenie logického prístupu

Okrem zabezpečenia samotnej fyzickej bezpečnosti systémov, je veľmi dôležité aj definovanie a následné zabezpečenie logického prístupu na jednotlivé sieťové prostriedky a servery (cez vzdialenú plochu, alebo niektorý zo sieťových protokolov).

- Skupiny s obmedzeným členstvom (Restricted Groups) – administrátor je schopný kontrolovať a riadiť členstvo v dôležitých lokálnych skupinách, na koncových staniciach a serveroch.
- Konfigurácia Brány Windows Firewall s pokročilými nastaveniami umožňuje:
    - *„Filtrovanie prichádzajúcej a odchádzajúcej dátovej komunikácie prostredníctvom protokolu IP verzie 4 (IPv4) a IP verzie 6 (IPv6)*
    - *Ochrana odosielaných a prijímaných dát pomocou protokolu Ipsec, za účelom overenia integrity sieťovej prevádzky, overenia identity počítačov alebo*

používateľov prijímajúcich, či odosielajúcich dáta a voliteľne taktiež pre zaistenie dôvernosti dát šifrovaním" [32].

2.3.5 Zabezpečenie dát

Operačný systém Windows ponúka solídne zabezpečenie dát uložených na súborovom systéme NTFS, či už na úrovni jednotlivých súborov, adresárov, alebo aj celého fyzického disku.

ACL, EFS, Bitlocker, alebo AD RMS?

- Access Control List (ACL) – zabezpečenie objektov v systéme Microsoft Windows prostredníctvom prepojených mechanizmov autentizácie a autorizácie. Windows Server používa autorizáciu užívateľa a zisťuje, či takýto užívateľ má oprávnenie k objektu, ktorý je chránený prostredníctvom práv ACL.
- Encrypted File System (EFS) – chráni citlivé dáta vo všetkých typoch súborov, ktoré sú uložené na súborovom systéme NTFS. Používa symetrický kľúč v kombinácii s technológiou PKI. V EFS, na rozdiel od väčšiny iných externých šifrovacích služieb, šifrovanie súborov nevyžaduje vlastníka súboru na dešifrovanie a opätovné zašifrovanie súboru pri každom použití. Tento proces sa vykonáva automaticky.
- Active Directory Rights Management Services (AD RMS) – hlavnou výhodou služby je to, že dokáže zabezpečiť vybrané typy súborov nielen v rámci vnútropodnikovej siete, ale aj mimo nej. Pomocou AD RMS je administrátor schopný na základe definovaných pravidiel úplne zamedziť, alebo presne definovať rôzne typy prístupu a tým aj práce s chráneným dokumentom. Užívateľ môže mať napríklad pridelené oprávnenia na čítanie, modifikovanie, tlač, alebo preposlanie súboru. Podmienkou nasadenia služby je existujúca PKI infraštruktúra a produkt vyžaduje zakúpenie dodatočných licencií.
- Bitlocker – „*Windows BitLocker Drive Encryption je funkcia pre ochranu dát, ktorá je k dispozícii v klientských systémoch od verzie Windows Vista a vo všetkých edíciách systému Windows Server 2008 a novších. Tento nástroj predstavuje novú funkciu od spoločnosti Microsoft a umožňuje reagovať na reálne hrozby odcudzenia dát alebo zverejnenia dát v prípade straty, odcudzenia alebo nezodpovedajúceho vyradenia počítačového hardvéru.*

Táto funkcia optimálne využíva technológiu Trusted Platform Module (TPM) 1.2 na ochranu dát a umožňuje zaistiť, aby s počítačom, v ktorom je prevádzkovaný systém, nebolo možné neoprávnene manipulovať v čase, kedy je systém offline. Nástroj Windows BitLocker Drive Encryption ponúka rozšírené šifrovanie dát vďaka kombinácii dvoch hlavných čiastkových funkcií: úplné šifrovanie jednotky a kontrola integrity súčastí používaných v prvých fázach spúšťania systému“ *[33]*.

Napriek tomu, že je odporúčané použiť na úschovu šifrovacích informácií TPM, je možné Bitlocker využiť aj v prípade, že daný systém TPM čip neobsahuje. Nevýhodou tohto riešenia je, že užívateľ musí definovať heslo, alebo uložiť informácie potrebné k dešifrovaniu na USB kľúč. Zvolené heslo je potom požadované pri každom štarte počítača. Ak užívateľ pri šifrovaní zvolil ako úložisko USB kľúč, tento musí byť pri každom štarte systému pripojený, inak sa užívateľ nedostane k obsahu šifrovaného disku.

Novou, zaujímavou funkcionalitou implementovanou v systémoch Microsoft Windows 7 a novších je Network Unlock. Funkcia zjednodušuje použitie tzv. viacnásobnej (multifaktor) ochrany pri Bitlocker šifrovaní. Informácie potrebné k dešifrovaniu obsahu disku sú uložené v TPM čipe, ale zároveň je systém pri svojom štarte chránený aj PIN kódom, ktorý si užívateľ zvolil, keď povolil šifrovanie daného disku. Pri štarte sa zariadenie automaticky snaží kontaktovať server, na ktorom sú nainštalované Network Unlock komponenty. Ak sa spojenie podarí nadviazať, zariadenia si navzájom vymenia potrebné informácie a užívateľ nemusí zadávať PIN pri štarte systému. V opačnom prípade (server je nedostupný, alebo je klient mimo korporátnej siete), musí užívateľ pri štarte systému zadať definovaný PIN kód.

- Bitlocker to go – je verziou Bitlocker aplikácie, určenou primárne na zabezpečenie prenosných a flash USB diskov. Uložené dáta sú šifrované heslom a správca si môže zvoliť, či povolí užívateľom aby si šifrovanie riadili sami, alebo bude pravidlá určovať organizácia centrálne, pomocou doménových skupinových politík.

3 UŽÍVATEĽSKÉ PROFILY

Profil užívateľa sa vytvára automaticky pri jeho prvotnom prihlásení na daný počítač. Každý užívateľ má jedinečný profil, ktorý v zásade obsahuje dva základné typy priečinkov:

- Priečinky, ktoré užívateľ štandardne vidí a vie používať – napr. kontakty, pracovná plocha, dokumenty, obľúbené položky, obrázky, videá, ...
- Systémové adresáre – aplikačné dáta, úložiská pre dočasné súbory, konfiguračné súbory jednotlivých aplikácií a iné [11, 46].

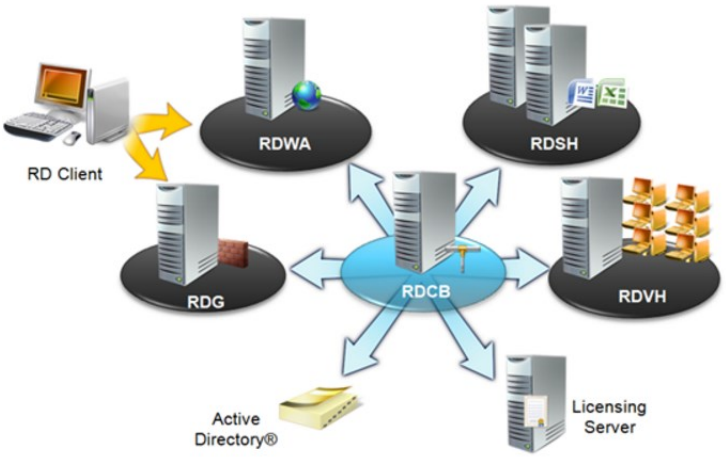
3.1 Typy užívateľských profilov

- Miestny užívateľský profil (Local Profile) – je platný iba v rámci daného počítača. Všetky nastavenia, ktoré užívateľ vykoná, ako napr. zmena pozadia, alebo nastavenie štart menu, majú vplyv iba na tento jeden konkrétny počítač a neprenášajú sa na iný počítač v sieti.
- Cestovný profil (Roaming Profile) – ako napovedá samotný názov, profil s užívateľom „cestuje“. Profil užívateľa je v skutočnosti uložený na zdieľanom sieťovom úložisku a pri prihlásení užívateľa sa automaticky prekopíruje na počítač, na ktorý sa užívateľ hlási. Pri odhlásení užívateľa, sa následne opäť vrátane všetkých vykonaných zmien automaticky skopíruje na dané sieťové úložisko.
- Povinný, alebo vynútený profil (Mandatory Profile) – je istým typom cestovného profilu. Na rozdiel od neho, však všetky zmeny, ktoré užívateľ vykoná, sú po jeho odhlásení sa zo systému „zahodené“. Užívateľ má pri každom novom prihlásení vždy rovnaké nastavenia – tie, ktoré definoval správca pri vytváraní profilu.
- Dočasný profil (Temporary Profile) – vytvára sa automaticky vždy, ak nie je možné načítať niektorý s vyššie uvedených užívateľských profilov. Dočasný profil sa po odhlásení užívateľa zo systému automaticky vymaže [11].

4 SLUŽBY VZDIALENEJ PLOCHY (RDS)

Služba Vzdialenej plochy (RDS), predtým označovaná aj ako Terminálová služba (Terminal Services), poskytuje technológie, ktoré umožňujú užívateľom používať aplikácie založené na Windows platforme nainštalované na vzdialenom servery, využívať všetky prostriedky vzdialeného servera cez vzdialenú plochu, alebo rovno celý dedikovaný vzdialený virtuálny počítač. Výhodou použitia RDS, je efektívne nasadzovanie a spravovanie softvérových prostriedkov v infraštruktúre zákazníka. Fakt, že jednotlivé programy a aplikácie sú nasadzované priamo na server a nie na jednotlivé pracovné stanice, zároveň zvyšuje bezpečnosť riešenia. V prípade objavenia zraniteľnosti, alebo chyby v aplikácii, nie je potrebné sa zaoberať veľkým počtom klientských staníc, ale iba servermi, kde je daná aplikácia nainštalovaná [34].

Ak má užívateľ prístup priamo na pracovnú plochu vzdialeného servera, všetky programy a aplikácie sa spúšťajú v kontexte a s oprávneniami daného užívateľa. Každý pripojený užívateľ pracuje vo svojej vlastnej izolovanej relácii (Session) [34, 43].



Obr. 9: Súčasti RDS infraštruktúry [35].

Základné súčasti RDS:

- Hostiteľ relácií vzdialenej plochy (RD Session Host Server) – je základnou rolou nevyhnutnou pre správnu funkcionalitu celého riešenia vzdialenej plochy. Priamo na tomto serveri sú nainštalované programy a aplikácie, ktoré chce neskôr správca poskytnúť užívateľom. Užívateľ sa pripája priamo na pracovnú plochu servera a využíva jeho výpočtový výkon, úložný priestor a sieťové prostriedky.
- Webový prístup vzdialenej plochy (RD Web Access) – umožňuje užívateľom pristupovať k aplikáciám a programom, ktoré im sprístupnil ich správca, cez webový prehliadač (napr. Internet Explorer), nainštalovaný na klientskej stanici [34, 43].
- Brána vzdialenej plochy (RD Gateway) – umožňuje autorizovaným užívateľom prístup na poskytované firemné programy a aplikácie z ľubovoľného zariadenia, pripojeného do internetu [34, 45].
- Licencovanie vzdialenej plochy (RDS Licensing) – spravuje licencie potrebné pre klientský prístup k službám vzdialenej plochy. Slúži k inštalácii, vydávaniu a kontrole dostupnosti licencií [34, 43, 45].

  Každý užívateľ, alebo zariadenie, ktoré chce využívať niektorý z komponentov RDS, potrebuje klientskú licenciu (CAL). Na základe zvoleného licenčného modelu, poznáme dva základné typy týchto licencií:

  - Licencia pre užívateľa (per User licensing) – každý užívateľ má svoju licenciu, spárovanú so svojim doménovým účtom. Aplikácie poskytované prostredníctvom služieb vzdialenej plochy môže využívať z ľubovoľného zariadenia v sieti.
  - Licencia pre zariadenie (per Device licensing) – licencia je priradená konkrétnemu zariadeniu. V tomto prípade nezáleží na tom, aký užívateľ sa z daného zariadenia na poskytované služby pripája.
- Sprostredkovateľ pripojenia k vzdialenej ploche (RD Connection Brooker) – služba sa využíva v prípade, že sa užívateľ pripája cez webové rozhranie. V prípade nasadenia viacerých hostiteľských serverov (RDS Session host farm), služba poskytuje riadenie záťaže[7] a správu relácií (napr. opätovné pripojenie užívateľa do jeho relácie, v prípade krátkodobého výpadku sieťovej komunikácie) [34, 43].

[7] Riadenie záťaže (Load Ballancing) – distribúcia prichádzajúcich užívateľských pripojení na základe zaťaženia konkrétneho hostiteľa relácií.

- Hostiteľ virtualizácie vzdialenej plochy (RD Virtualization Host) – v spolupráci s virtualizačnou technológiou Hyper-V, slúži k hosťovaniu virtuálnych počítačov a ich následnému poskytnutiu koncovým užívateľom. Každému užívateľovi vo svojej organizácii je možné priradiť dedikovanú virtuálnu pracovnú stanicu[8], alebo zdieľaný prístup na skupinu virtuálnych pracovných staníc [34, 45].

[8] Pod pojmom virtuálna pracovná stanica, rozumieme kompletne nainštalovaný a nakonfigurovaný virtuálny počítač (napr. Windows 10), s predinštalovanými všetkými požadovanými firemnými aplikáciami.

5 OSTATNÉ DÔLEŽITÉ ROLE A SLUŽBY

5.1 Domain Name System (DNS)

DNS je protokol určený na preklad názvov v TCP/IP sieťach. DNS server má vo svojej databáze uložené informácie, ktoré klientovi umožňujú preklad ťažšie zapamätateľnej číselnej hodnoty (IP adresy) na alfanumerický názov a opačne [36].

5.2 Dynamic Host Configuration Protocol (DHCP)

DHCP je služba nainštalovaná na serveri, ktorá TCP/IP klientom (počítač, server a iné sieťové zariadenia) automaticky poskytuje TCP/IP nastavenia, ako sú IP adresa, maska podsiete, predvolená brána, DNS, či WINS servery [37].

5.3 Súborové a Tlačové Služby (File and Print services)

Súborový server je spoľahlivé sieťové úložisko užívateľských a aplikačných dát. Zároveň môže plniť úlohy ako zabezpečenie, indexácia, nastavovanie kvót, či zdieľanie uloženého obsahu [38].

Tlačový server, slúži na zdieľanie nainštalovaných tlačiarní jednotlivým užívateľom pripojeným vo firemnej sieti. Tlačové fronty sú tak centrálne spravované, monitorované a aktualizované.

5.4 Windows Server Update Services (WSUS)

„ WSUS je služba zaisťujúca aktualizáciu softvéru pre operačné systémy Microsoft Windows. Služba je lokálne spravovanou alternatívou ku službe Microsoft Update. WSUS umožňuje správcom nasadzovať najnovšie aktualizácie Microsoft produktov na počítače, s podporovaným operačným systémom z jedného centrálneho servera umiestneného vo firemnej sieti" [38].

6 KLIENTSKÁ STANICA (TENKÝ KLIENT)

Čo je vlastné tenký klient?

Pod pojmom tenký klient väčšinou rozumieme malý, jednoúčelový počítač, ktorý je vybavený iba minimálnym hardvérom nutným na pripojenie sa na sieťový server. V prípade tenkého klienta, hardvérové parametre nie sú primárnym parametrom. Tenký klient využíva výpočtový výkon sieťového servera, ku ktorému sa pripája jedným zo štandardných sieťových protokolov.

Medzi hlavné **výhody** tenkých klientov patria:

- Jednoduchšie spravovanie – v porovnaní s klasickým počítačom, je na tenkom klientovi nainštalovaná iba základná sada programov nevyhnutných na pripojenie sa na vzdialený server. Programy, ako aj samotný operačný systém, bývajú väčšinou na pamäťovom médiu, ktoré je chránené proti zápisu.
- Dlhšia životnosť – tenký klient často neobsahuje pevný disk, ani žiadne ďalšie pohyblivé súčasti, kde je väčšia pravdepodobnosť výskytu poruchy. Je preto vhodným kandidátom do extrémnejšieho prostredia, ako sú napr. výrobné haly, prašné prostredie a podobne.
- Bezpečnosť – klient štandardne neobsahuje CD, či DVD mechaniku a USB porty môže administrátor takisto zakázať, či obmedziť iba na určitý typ zariadení, ako napr. tlačiarne. Keďže bežný užívateľ nemá oprávnenia na zápis na úložisko s operačným systémom a aplikáciami, nie je schopný vykonávať žiadne softvérové zmeny.
- Vstupné a prevádzkové náklady – vstupné náklady na tenkého klienta sú o niečo vyššie ako náklady na lacnejšiu pracovnú stanicu. Ak sa však zameriame na dlhodobé náklady, situácia sa mení: *„Podľa analytických agentúr sú náklady na administráciu tenkého klienta v porovnaní s „péčéčkom“ o tretinu až polovicu nižšie. Analýza Forrester Research ukázala, že výraznejšie úspory možno dosiahnuť po úplnom prechode na tenkých klientov než v heterogénnom prostredí, kde majú zastúpenie aj desktopové PC. Ďalšie výhody pramenia z úspory elektrickej energie. Kým bežné PC spotrebuje 80 wattov, Sun Ray iba 13 wattov“ [39].*

Nevýhody tenkých klientov:

- Kompatibilita aplikácii a hardvérového vybavenia – niektoré aplikácie nie je možné využívať v spojení so servermi vzdialenej plochy a nie všetky hardvérové komponenty sú podporované na operačných systémoch, ktoré bežia na tenkých klientoch.
- Vstupné investície – ak organizácia využíva neznačkové osobné počítače, prípadne si počítače sama kompletizuje zo zakúpených komponentov, môže byť cena tenkého klienta privysoká.

Obr. 10: Tenký Klient - Dell Wyse 7000 [40].

II. PRAKTICKÁ ČASŤ

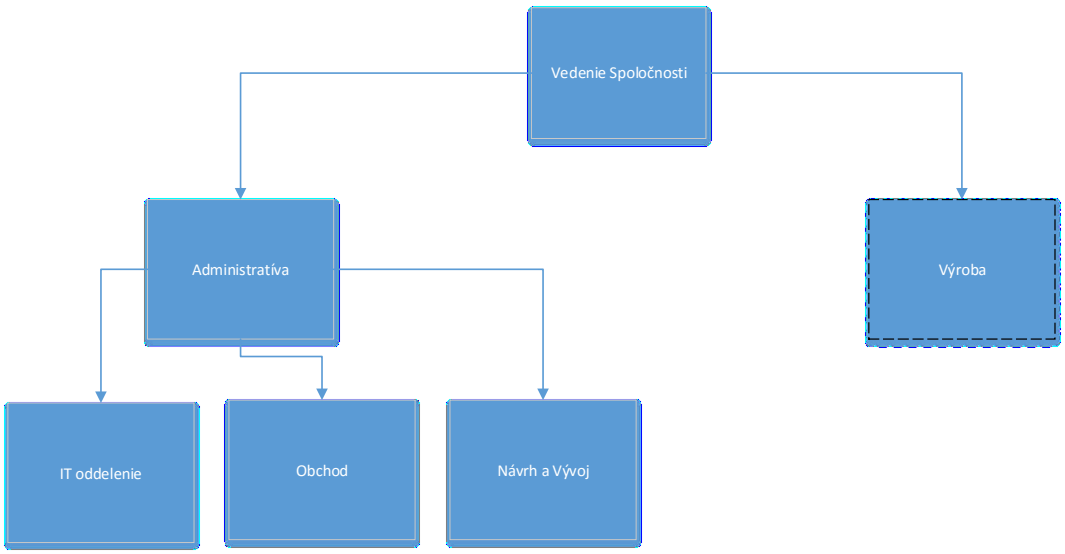
7 POPIS SÚČASNÉHO STAVU

V súčasnosti fiktívna spoločnosť KVAIT s.r.o. zamestnáva 80 zamestnancov. Firma má výrobnú a administratívnu divíziu. V administratíve pracuje 60 zamestnancov, ostatní pracujú vo výrobe. Spoločnosť sa zaoberá návrhom, vývojom a výrobou náhradných dielov pre poľnohospodárske zariadenia a vo svojom objekte má dve výrobné haly.

Všetky pracovné stanice sú zaradené do domény a každý užívateľ má svoj personalizovaný účet v AD. Spoločnosť prevádzkuje väčšinu svojich serverov vo virtuálnom prostredí a to na virtualizačnej platforme VMWare.

7.1 Organizačná štruktúra spoločnosti

Organizačná štruktúra Active Directory odráža reálnu organizačnú štruktúru spoločnosti.



Obr. 11: Organizačná štruktúra spoločnosti, vlastný zdroj.

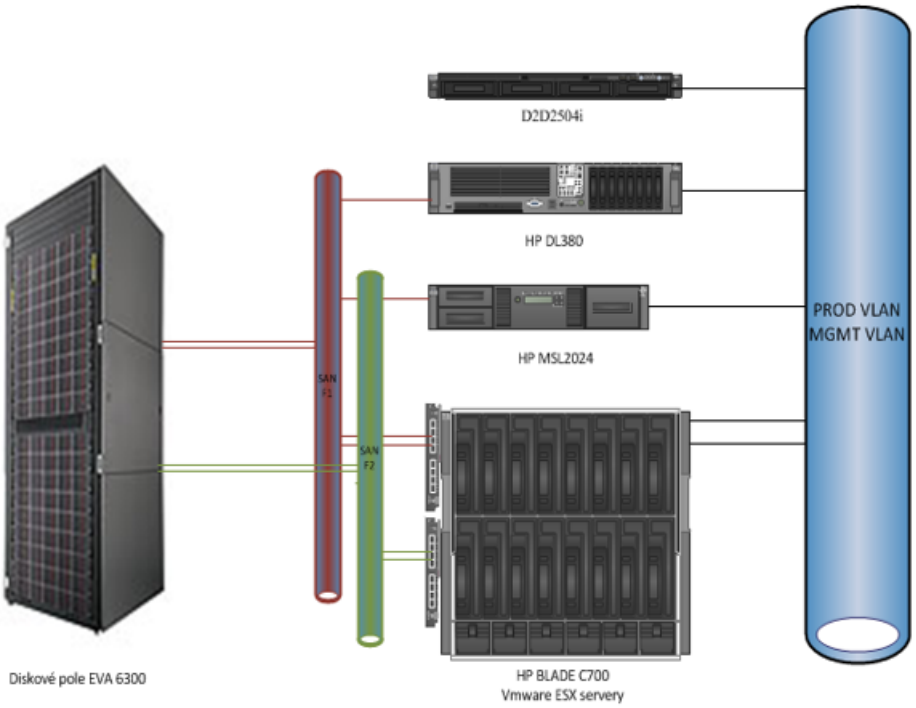
Organizačné jednotky sú ďalej členené podľa jednotlivých typov uložených objektov (počítače, servery, skupiny, užívatelia, tlačiarne a zdieľané prostriedky).

Adresárové služby poskytujú dva doménové radiče s operačným systémom Windows Server 2012 R2. Funkčný level domény aj celého lesa je Windows Server 2012 R2.

7.2 HW infraštruktúra spoločnosti

Použitá VMware virtualizačná platforma je založená na HP C700 Blade serveroch. Vysoká dostupnosť je zabezpečená na úrovni ESX serverov. Pomocou technológie Vmotion je v prípade výpadku jedného z VMware severov, zabezpečený presun virtuálnych serverov na druhý ESX server. Virtuálne servery boli nainštalované zo šablóny operačných systémov Windows Server 2008 R2 a Windows Server 2012 R2.

Fyzický server srvbck01 slúži ako zálohovací a manažment server. Nachádzajú sa tu nástroje pre správu diskového poľa a ESX farmy.



Obr. 12: Komponenty HW infraštruktúry, vlastný zdroj.

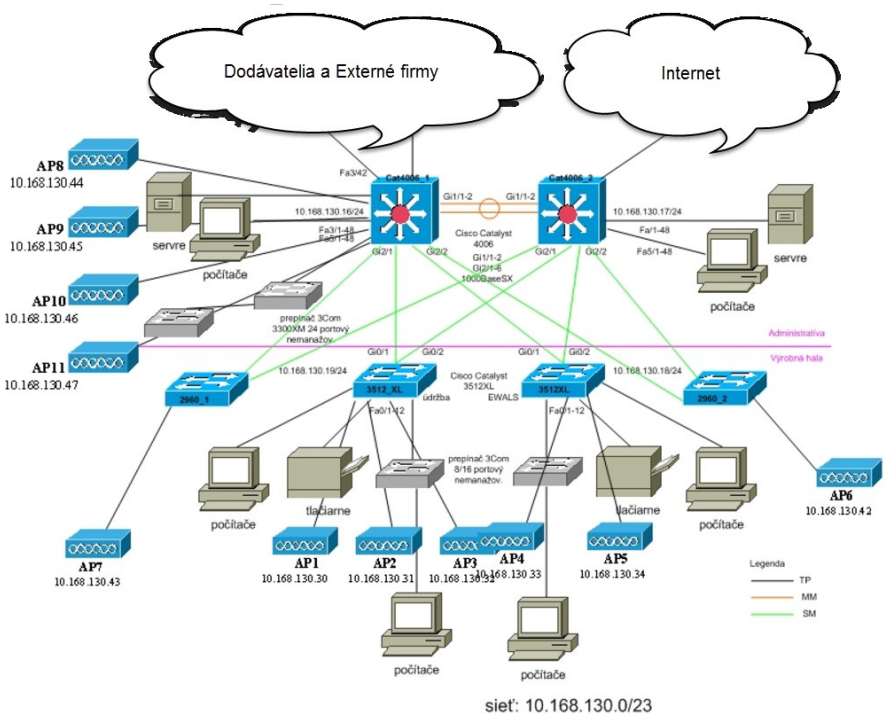
7.3 Zoznam Serverov a služieb

Názov	Fyzický/Virtuálny server	IP adresa	Aplikácia/Rola
esx01.kvait.local	Fyzický	10.168.128.96	VMWare ESX server
esx02.kvait.local	Fyzický	10.168.128.97	VMWare ESX server
srvbck01.kvait.local	Fyzický	10.168.128.105	Zálohovací a manažment server
ad01.kvait.local	Virtuálny	10.168.128.101	Doménový radič, DHCP, DNS
ad02.kvait.local	Virtuálny	10.168.128.102	Doménový radič, DHCP, DNS
srvfile02.kvait.local	Virtuálny	10.168.128.103	Súborový server
srvrds01.kvait.local	Virtuálny	10.168.128.104	RDS server
srvapp01.kvait.local	Virtuálny	10.168.128.106	Aplikačný server, IIS
srvapp02.kvait.local	Virtuálny	10.168.128.107	Aplikačný server
Srvapp03.kvait.local	Virtuálny	10.168.128.108	Aplikačný server
srvsql01.kvait.local	Virtuálny	10.168.128.109	Databázový server
srvmng01.kvait.local	Virtuálny	10.168.128.110	WSUS, ESET Remote Administrator

Tab. 4: Zoznam serverov a rolí, vlastný zdroj.

7.4 Sieťová topológia

Sieťovú vrstvu tvoria Cisco Catalyst prepínače 2960 a kostrové L3 stacky 3750. Bezdrôtová sieť pozostáva z 12ks autonómnych prístupových bodov.



Obr. 13: Sieťová topológia, vlastný zdroj.

8 CIELE NÁVRHU A POŽIADAVKY SPOLOČNOSTI

- Zamedziť úniku dát vo výrobe
  - Zamedziť spúšťaniu a inštalácii nepovolených aplikácií na klientskej stanici.
  - Zamedziť možnosti konfigurácie klientskej stanice bežným užívateľom.
  - Zamedziť používaniu USB prenosných diskov a zariadení.
  - Minimalizácia úniku firemných dát, v prípade odcudzenia počítača vo výrobe.
- Zníženie poruchovosti počítačov vo výrobe.
- Zvýšenie bezpečnosti citlivých údajov na súborovom serveri.
- Jednotná konfigurácia užívateľskej pracovnej plochy.
- Centralizovaná a zjednodušená administrácia počítačov a užívateľov.
- Zjednodušená správa a aktualizácia definovaných aplikácií.

9 NASADENÉ RIEŠENIE

Základom navrhovaného riešenia, bola existujúca infraštruktúra spoločnosti, ktorá bola rozšírená o potrebné komponenty a systémy. Rola RDS zo všetkými potrebnými súčasťami, bola nainštalovaná na novom virtuálnom serveri, s operačným systémom Microsoft Windows Server 2012 R2 Standard. Na serveri boli zároveň nainštalované zákazníkom definované aplikácie.

Bežný pracovníci, pripájajúci sa na server, majú zamedzený prístup ku konfiguračným nastaveniam jednotlivých aplikácií, ako aj samotného systému. Na tento účel sa využívajú doménové politiky a nastavenia register databázy. Každému užívateľovi sa automaticky mapujú zdieľané disky zo súborového servera, kde sú uložené výrobné výkresy.

Na tenkom klientovi má užívateľ zamedzený prístup ku konfiguračným zmenám a jediná aplikácia, ktorú je schopný spustiť je Remote desktop klient, ktorým sa pripája na pracovnú plochu RDS servera.

9.1 Súborový server

Na existujúcom súborovom serveri bol vytvorený zdieľaný adresár, ktorý slúži ako sieťové úložisko pre správcom nakonfigurovaný **mandatory** užívateľský profil. Profil sa aplikuje vždy, keď sa na RDS server prihlási užívateľ s obmedzenými oprávneniami a zabezpečí, aby užívateľ mal vždy rovnaké nastavenia užívateľského rozhrania.

Bezpečnosť dát

Dáta na súborovom serveri sú zabezpečené pomocou ACL. Adresárová štruktúra a ukladané dáta sú členené na základe organizačnej štruktúry spoločnosti. Prístup do jednotlivých priečinkov je riadený na základe členstva v prislúchajúcej doménovej globálnej skupine.

Na monitorovanie zmien vykonaných na citlivých údajoch uložených v priečinku vedenia spoločnosti, bolo nasadené podrobné auditovanie. V prípade neautorizovaného prístupu, alebo modifikácie dát, bude možné spätne dohľadať všetky potrebné informácie.

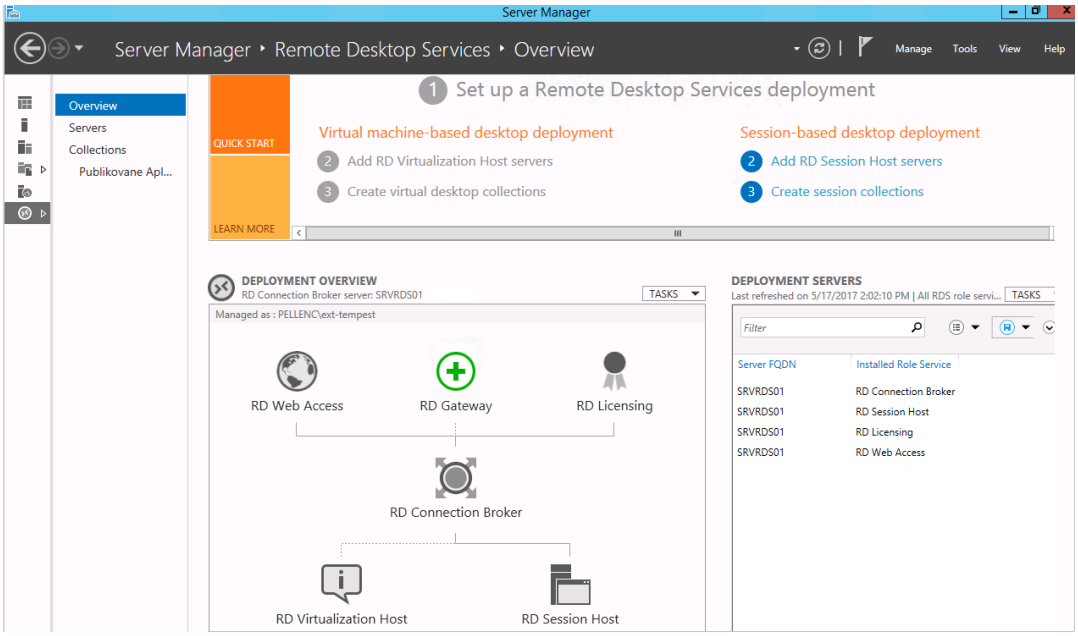
Ďalšie zvýšenie bezpečnosti uložených údajov by priniesla implementácia Bitlocker, EFS a AD RMS. To však vzhľadom na systémové a hardvérové požiadavky týchto technológií, nie je v spoločnosti KVAIT možné.

9.2 RDS server

Pre potreby spoločnosti bol zvolený model s jedným RDS serverom, s nainštalovanými rolami: RD Connection Brooker, RD Session Host, RD Licensing a RD Web Access.

Na server boli nainštalované aplikácie: Adobe Acrobat Reader, Eset antivírus, eDrawings2015 a aplikácia na tlačenie štítkov.

Užívatelia sa na RDS server pripájajú pomocou Remote desktop klient aplikácie, štandardne vstavanej vo Windows operačnom systéme.



Obr. 14: Role RDS, vlastný zdroj.

9.2.1 Hardvérové parametre a použité licencie

Licencie potrebné pre server samotný a 20 užívateľov súčasne pracujúcich na novom RDS serveri:

Počet	Licencia
1	Windows Server 2012 R2 Standard
20	RDS device CAL

Tab. 5: RDS server – použité licencie, vlastný zdroj.

Odhad potrebných hardvérových prostriedkov:

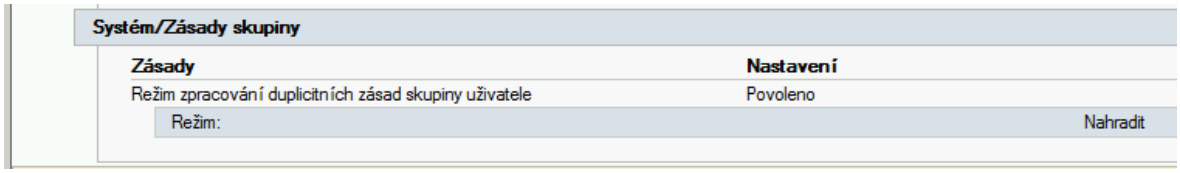
Komponent	Parametre
Procesor	2 jadrá
Operačná Pamäť	12 GB
Pevný Disk	60 GB

Tab. 6: RDS server – hardvérové parametre, vlastný zdroj.

9.3 AD infraštruktúra

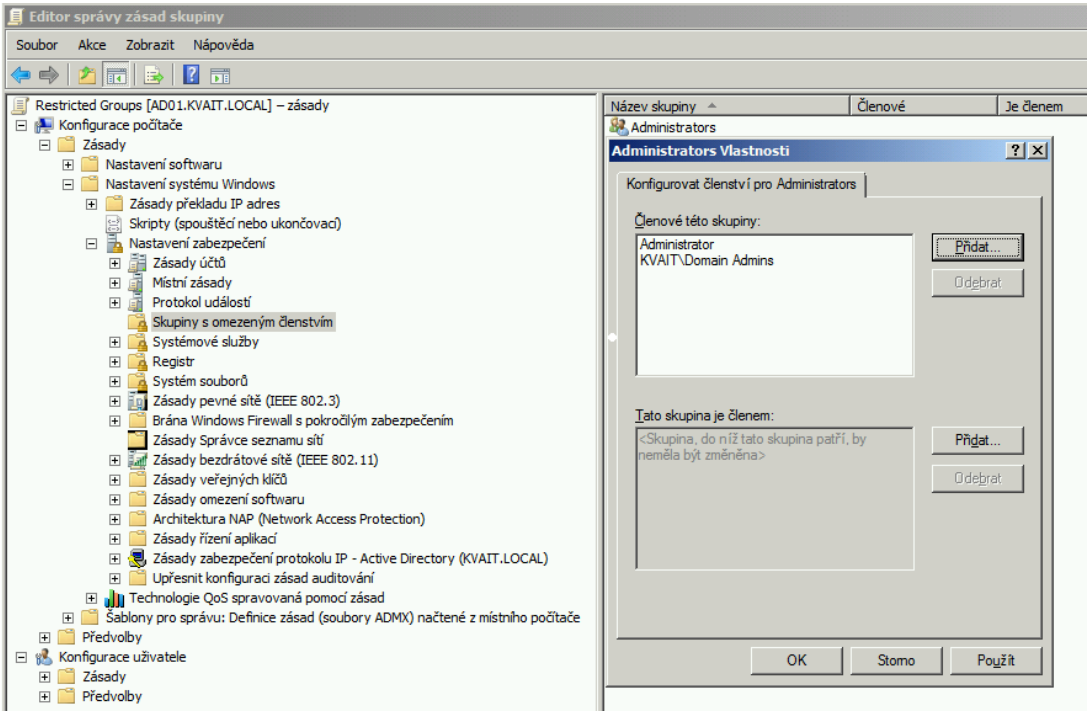
V existujúcej Active Directory infraštruktúre boli vytvorené dve nové skupinové politiky a jedna globálna užívateľská skupina:

- Globálna skupina (názov: RDS Users) – skupina, v ktorej sa nachádzajú užívatelia s obmedzenými oprávneniami, ktorí budú pracovať na RDS serveri.
- Skupinová politika s názvom **RDS Settings** – politika definuje nastavenia pre užívateľa aj samotný server. Aby bolo zabezpečené, že nastavenia politiky aplikované na počítač, prepíšu všetky potenciálne konfliktné nastavenia aplikované inými priradenými politikami, bol nakonfigurovaný „Režim spracovania duplicitných zásad skupiny užívateľa“ na „Nahradiť“.



Obr. 15: Režim spracovania duplicitných zásad skupiny užívateľa, vlastný zdroj.

- Skupinová politika s názvom **Restricted group** – politika zabezpečí, aby na serveri lokálna skupina Administrátors, obsahovala iba užívateľov a doménové skupiny, ktoré definoval doménový správca.



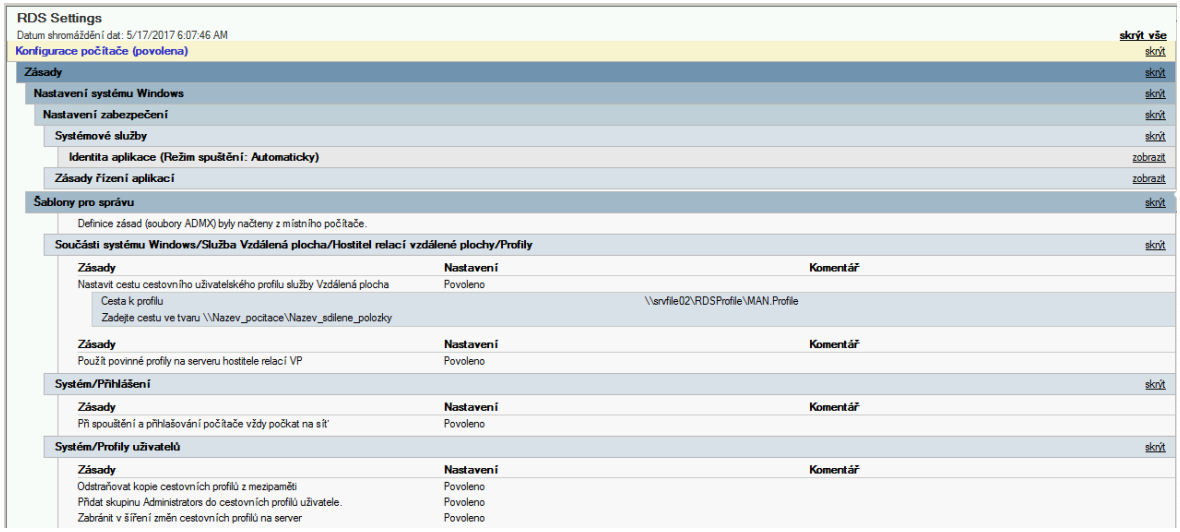
Obr. 16: Konfigurácia skupín s obmedzeným členstvom, vlastný zdroj.

9.4 Doménová skupinová politika – RDS Settings

RDS Settings politika, je základným prvkom zabezpečenia implementovaných RDS služieb. Jednotlivé skupiny nastavení sú rozdelené do kategórií, z ktorých každá ovplyvňuje inú časť systému.

9.4.1 Konfigurácia profilu

Cieľom doménového správcu bolo zaistiť, aby každý užívateľ, ktorý sa pripojí na RDS server, mal rovnako nakonfigurované svoje užívateľské rozhranie. Zároveň bolo požadované, aby užívateľ vo svojom profile nemohol vykonávať žiadne zmeny. Spoločný mandatory profil sa preto pri každom prihlásení na RDS server načíta zo súborového servera a pri každom odhlásení užívateľa, sa zo servera automaticky zmaže.



RDS Settings

Datum shromáždění dat: 5/17/2017 6:07:46 AM — skrýt vše

Konfigurace počítače (povolena) — skrýt

Zásady — skrýt

Nastavení systému Windows — skrýt

Nastavení zabezpečení — skrýt

Systémové služby — skrýt

Identita aplikace (Režim spuštění: Automaticky) — zobrazit

Zásady řízení aplikací — zobrazit

Šablony pro správu — skrýt

Definice zásad (soubory ADMX) byly načteny z místního počítače.

Součásti systému Windows/Služba Vzdálená plocha/Hostitel relací vzdálené plochy/Profily — skrýt

Zásady	Nastavení	Komentář
Nastavit cestu cestovního uživatelského profilu služby Vzdálená plocha	Povoleno	
Cesta k profilu Zadejte cestu ve tvaru \\Nazev_pocitace\Nazev_sdilene_polozky	\\srvfile02\RDSProfile\MAN.Profile	

Zásady	Nastavení	Komentář
Použít povinné profily na serveru hostitele relací VP	Povoleno	

Systém/Přihlášení — skrýt

Zásady	Nastavení	Komentář
Při spouštění a přihlašování počítače vždy počkat na síť	Povoleno	

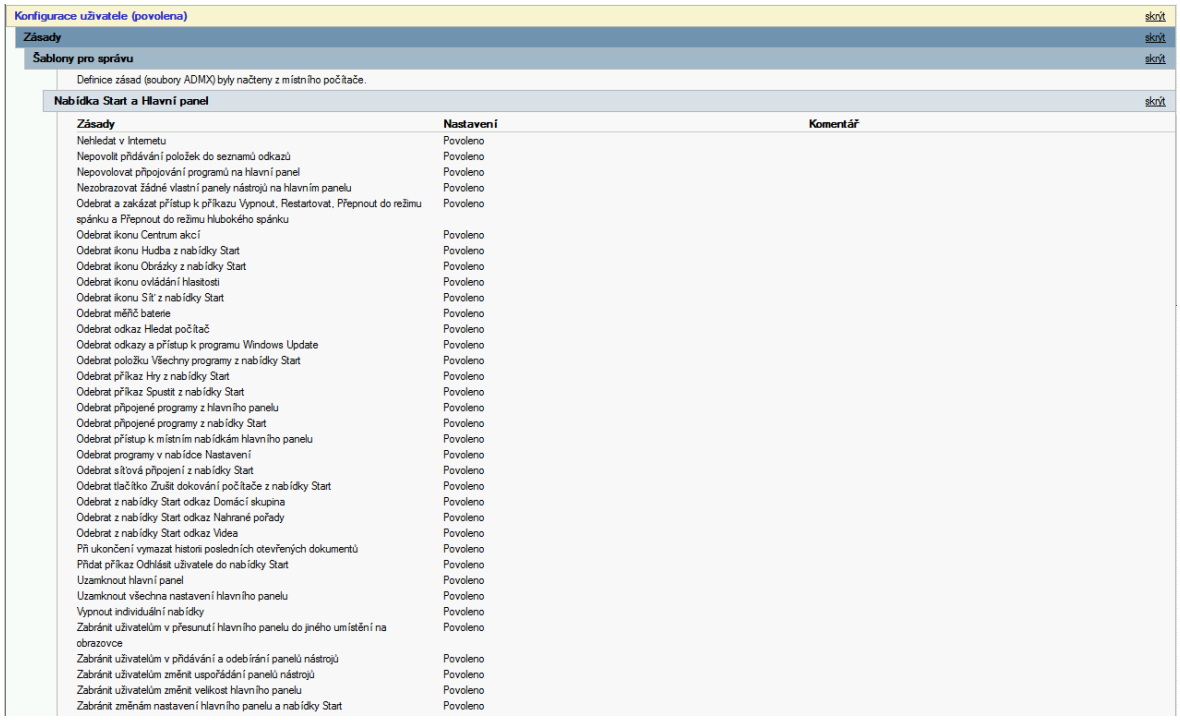
Systém/Profily uživatelů — skrýt

Zásady	Nastavení	Komentář
Odstraňovat kopie cestovních profilů z mezipaměti	Povoleno	
Přidat skupinu Administrators do cestovních profilů uživatele.	Povoleno	
Zabránit v šíření změn cestovních profilů na server	Povoleno	

Obr. 17: Konfigurácia profilu, vlastný zdroj.

9.4.2 Ponuka štart a Hlavný panel

Táto skupina nastavení modifikuje vzhľad a obsah Štart ponuky. Postupne boli zakázané všetky ikony, odkazy a položky, ktoré nie sú nevyhnutne potrebné k práci bežného užívateľa.



Konfigurace uživatele (povolena) — skrýt

Zásady — skrýt

Šablony pro správu — skrýt

Definice zásad (soubory ADMX) byly načteny z místního počítače.

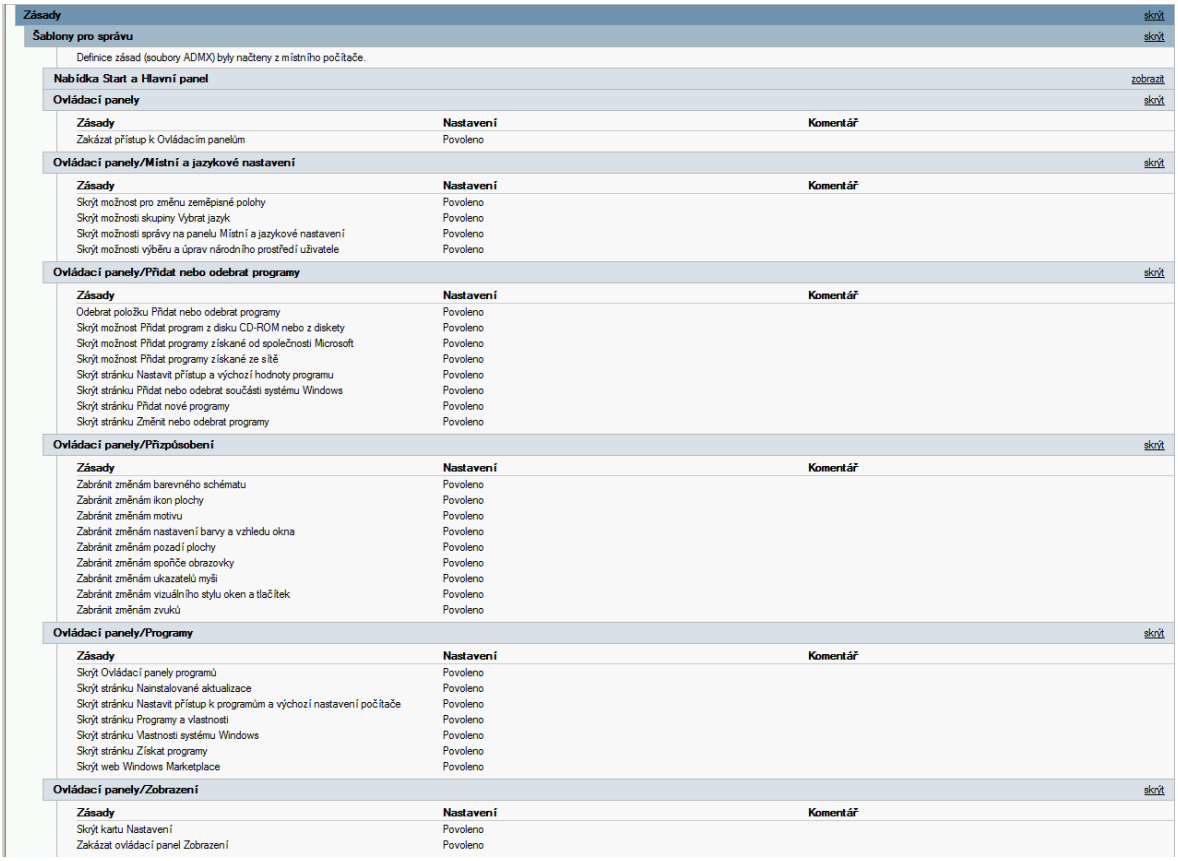
Nabídka Start a Hlavní panel — skrýt

Zásady	Nastavení	Komentář
Nehledat v Internetu	Povoleno	
Nepovolit přidávání položek do seznamů odkazů	Povoleno	
Nepovolovat připojování programů na hlavní panel	Povoleno	
Nezobrazovat žádné vlastní panely nástrojů na hlavním panelu	Povoleno	
Odebrat a zakázat přístup k příkazu Vypnout, Restartovat, Přepnout do režimu spánku a Přepnout do režimu hlubokého spánku	Povoleno	
Odebrat ikonu Centrum akcí	Povoleno	
Odebrat ikonu Hudba z nabídky Start	Povoleno	
Odebrat ikonu Obrázky z nabídky Start	Povoleno	
Odebrat ikonu ovládání hlasitosti	Povoleno	
Odebrat ikonu Síť z nabídky Start	Povoleno	
Odebrat měřič baterie	Povoleno	
Odebrat odkaz Hledat počítač	Povoleno	
Odebrat odkazy a přístup k programu Windows Update	Povoleno	
Odebrat položku Všechny programy z nabídky Start	Povoleno	
Odebrat příkaz Hry z nabídky Start	Povoleno	
Odebrat příkaz Spustit z nabídky Start	Povoleno	
Odebrat připojené programy z hlavního panelu	Povoleno	
Odebrat připojené programy z nabídky Start	Povoleno	
Odebrat přístup k místním nabídkám hlavního panelu	Povoleno	
Odebrat programy v nabídce Nastavení	Povoleno	
Odebrat síťová připojení z nabídky Start	Povoleno	
Odebrat tlačítko Zrušit dokování počítače z nabídky Start	Povoleno	
Odebrat z nabídky Start odkaz Domácí skupina	Povoleno	
Odebrat z nabídky Start odkaz Nahrané pořady	Povoleno	
Odebrat z nabídky Start odkaz Videa	Povoleno	
Při ukončení vymazat historii posledních otevřených dokumentů	Povoleno	
Přidat příkaz Odhlásit uživatele do nabídky Start	Povoleno	
Uzamknout hlavní panel	Povoleno	
Uzamknout všechna nastavení hlavního panelu	Povoleno	
Vypnout individuální nabídky	Povoleno	
Zabránit uživatelům v přesunutí hlavního panelu do jiného umístění na obrazovce	Povoleno	
Zabránit uživatelům v přidávání a odebírání panelů nástrojů	Povoleno	
Zabránit uživatelům změnit uspořádání panelů nástrojů	Povoleno	
Zabránit uživatelům změnit velikost hlavního panelu	Povoleno	
Zabránit změnám nastavení hlavního panelu a nabídky Start	Povoleno	

Obr. 18: Ponuka štart a Hlavný panel – nastavenia, vlastný zdroj.

9.4.3 Ovládacie panely

Všetky položky Ovládacích panelov boli ukryté a boli zakázané zmeny týkajúce sa prispôsobenia systému, ako napr. zmeny zvukov, šetriča obrazovky, ukazovateľov myši, či motívov.



Zásady			skrýt
Šablony pro správu			skrýt
Definice zásad (soubory ADMX) byly načteny z místního počítače.			
Nabídka Start a Hlavní panel			zobrazit
Ovládací panely			skrýt
Zásady	**Nastavení**	**Komentář**	
Zakázat přístup k Ovládacím panelům	Povoleno		
Ovládací panely/Místní a jazykové nastavení			skrýt
Zásady	**Nastavení**	**Komentář**	
Skrýt možnost pro změnu zeměpisné polohy	Povoleno		
Skrýt možnosti skupiny Vybrat jazyk	Povoleno		
Skrýt možnosti správy na panelu Místní a jazykové nastavení	Povoleno		
Skrýt možnosti výběru a úprav národního prostředí uživatele	Povoleno		
Ovládací panely/Přidat nebo odebrat programy			skrýt
Zásady	**Nastavení**	**Komentář**	
Odebrat položku Přidat nebo odebrat programy	Povoleno		
Skrýt možnost Přidat program z disku CD-ROM nebo z diskety	Povoleno		
Skrýt možnost Přidat programy získané od společnosti Microsoft	Povoleno		
Skrýt možnost Přidat programy získané ze sítě	Povoleno		
Skrýt stránku Nastavit přístup a výchozí hodnoty programu	Povoleno		
Skrýt stránku Přidat nebo odebrat součásti systému Windows	Povoleno		
Skrýt stránku Přidat nové programy	Povoleno		
Skrýt stránku Změnit nebo odebrat programy	Povoleno		
Ovládací panely/Přizpůsobení			skrýt
Zásady	**Nastavení**	**Komentář**	
Zabránit změnám barevného schématu	Povoleno		
Zabránit změnám ikon plochy	Povoleno		
Zabránit změnám motivu	Povoleno		
Zabránit změnám nastavení barvy a vzhledu okna	Povoleno		
Zabránit změnám pozadí plochy	Povoleno		
Zabránit změnám spořiče obrazovky	Povoleno		
Zabránit změnám ukazatelů myši	Povoleno		
Zabránit změnám vizuálního stylu oken a tlačítek	Povoleno		
Zabránit změnám zvuků	Povoleno		
Ovládací panely/Programy			skrýt
Zásady	**Nastavení**	**Komentář**	
Skrýt Ovládací panely programů	Povoleno		
Skrýt stránku Nainstalované aktualizace	Povoleno		
Skrýt stránku Nastavit přístup k programům a výchozí nastavení počítače	Povoleno		
Skrýt stránku Programy a vlastnosti	Povoleno		
Skrýt stránku Vlastnosti systému Windows	Povoleno		
Skrýt stránku Získat programy	Povoleno		
Skrýt web Windows Marketplace	Povoleno		
Ovládací panely/Zobrazení			skrýt
Zásady	**Nastavení**	**Komentář**	
Skrýt kartu Nastavení	Povoleno		
Zakázat ovládací panel Zobrazení	Povoleno		

Obr. 19: Ovládacie panely – nastavenia, vlastný zdroj.

9.4.4 Pracovná plocha

Výslednú podobu užívateľskému rozhraniu, ktoré užívateľ vidí, po svojom prihlásení sa na server, dáva kombinácia skupinovej politiky a administrátorom definovaného mandatory profilu.

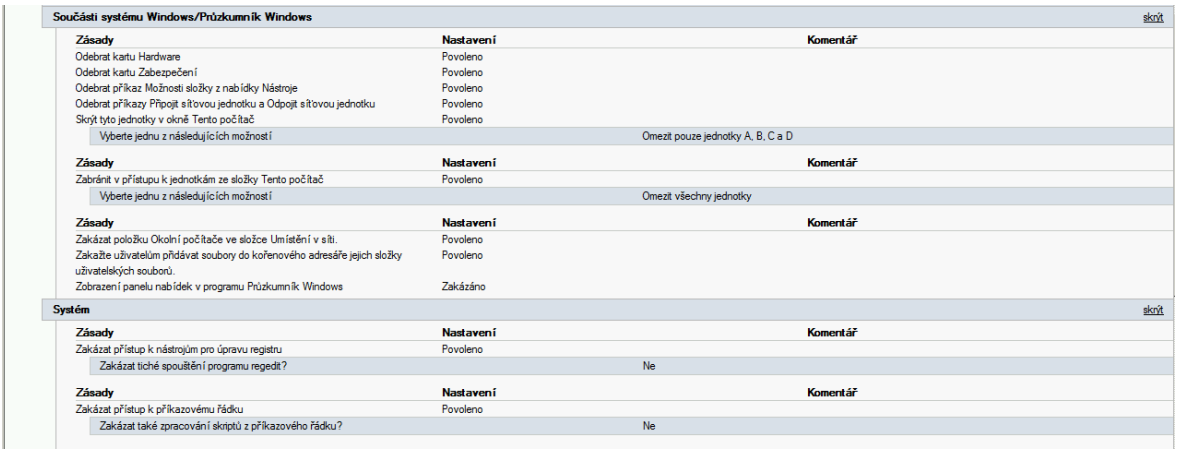
Plocha skrýt

Zásady	Nastavení	Komentář
Odebrat ikonu Koš z plochy	Povoleno	
Odebrat ikonu Počítač z plochy	Povoleno	
Odebrat příkaz Vlastnosti z místní nabídky ikony Dokumenty	Povoleno	
Odebrat příkaz Vlastnosti z místní nabídky ikony Počítač	Povoleno	
Skrytí ikony Umístění v síti na ploše	Povoleno	
Zakázat úpravy panelů nástrojů na ploše	Povoleno	
Zakázat uživatelům ručně přesměrovat složky profilů	Povoleno	

Obr. 20: Pracovná plocha – nastavenia, vlastný zdroj.

9.4.5 Prieskumník a Systém

Dôležitá časť celkového zabezpečenia vzdialenej plochy na RDS serveri. V časti Prieskumník systému Windows, boli z kontextového menu odstránené záložky Zabezpečenie a Hardvér. Bol zamedzený prístup k diskovej jednotke C a zakázané spúšťanie príkazového riadku a editoru registry databázy.



Součásti systému Windows/Průzkumník Windows skrýt

Zásady	Nastavení	Komentář
Odebrat kartu Hardware	Povoleno	
Odebrat kartu Zabezpečení	Povoleno	
Odebrat příkaz Možnosti složky z nabídky Nástroje	Povoleno	
Odebrat příkazy Připojit síťovou jednotku a Odpojit síťovou jednotku	Povoleno	
Skrýt tyto jednotky v okně Tento počítač	Povoleno	
Vyberte jednu z následujících možností	Omezit pouze jednotky A, B, C a D	
Zásady	**Nastavení**	**Komentář**
Zabránit v přístupu k jednotkám ze složky Tento počítač	Povoleno	
Vyberte jednu z následujících možností	Omezit všechny jednotky	
Zásady	**Nastavení**	**Komentář**
Zakázat položku Okolní počítače ve složce Umístění v síti.	Povoleno	
Zakažte uživatelům přidávat soubory do kořenového adresáře jejich složky uživatelských souborů.	Povoleno	
Zobrazení panelu nabídek v programu Průzkumník Windows	Zakázáno	

Systém skrýt

Zásady	Nastavení	Komentář
Zakázat přístup k nástrojům pro úpravu registru	Povoleno	
Zakázat tiché spouštění programu regedit?	Ne	
Zásady	**Nastavení**	**Komentář**
Zakázat přístup k příkazovému řádku	Povoleno	
Zakázat také zpracování skriptů z příkazového řádku?	Ne	

Obr. 21: Prieskumník systému Windows a položky Systém – nastavenia, vlastný zdroj.

9.4.6 Applocker

Jednotlivé skupiny užívateľov majú na základe definovaných pravidiel povolené, resp. zakázané spúšťanie aplikácií.

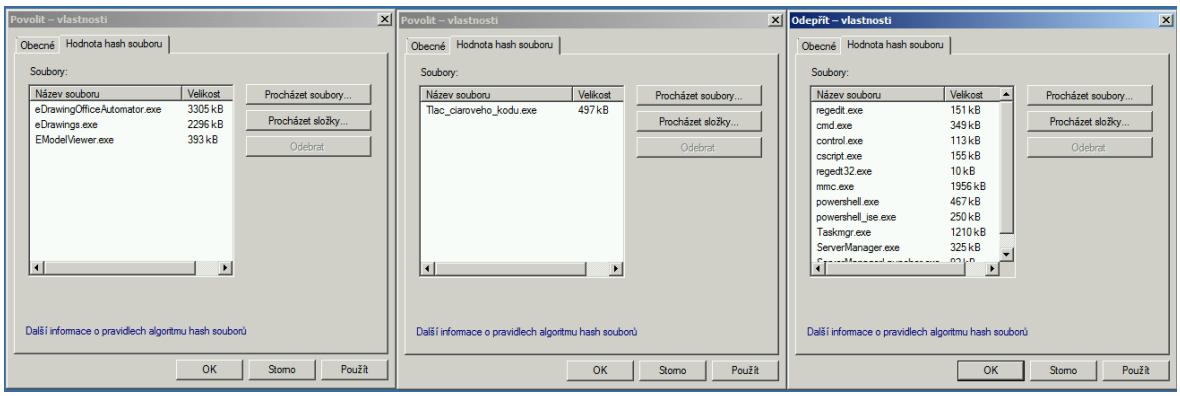
Skupina **Everyone** (všetci užívatelia) – ak aplikácia spadá pod definovaného **Vydavateľa,** je možné ju spustiť. Toto pravidlo povoľuje spustenie základných súčastí operačného systému. Na základe H**ash** hodnoty súboru, boli povolené zoznamy dodatočných systémových komponentov (.NET Framework, ...) a požadovaných aplikácií ako ESET antivírus, Adobe Acrobat Reader, eDrawing, atď.

Skupina **Administrátori** – použité boli predvolené konfiguračné pravidlá. Na túto skupinu sa nevzťahujú žiadne obmedzenia v súvislosti so spúšťaním aplikácií.

Akce	Uživatel	Název	Podmínka	Výjimky
Povolit	Everyone	System32: MICROSOFT PINYIN IME 2012 signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	System32: MICROSOFT® WINDOWS® OPERATING SYSTEM signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	EGUI.EXE, version 4.5.0.0 and above, in ESET FILE SECURITY FOR MICROSOFT WINDOWS SERVER, from O=ESET, SPOL. S R.O., L=BRATISLAVA, S=SLOVAKIA, C=SK	Vydavatel	
Povolit	Everyone	System32: MICROSOFT ® WINDOWS SCRIPT HOST signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	System32: MICROSOFT WINDOWS MALICIOUS SOFTWARE REMOVAL TOOL signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	VMTOOLSD.EXE, version 9.4.0.0 and above, in VMWARE TOOLS, from O=VMWARE, INC., L=PALO ALTO, S=CALIFORNIA, C=US	Vydavatel	
Povolit	Everyone	System32: INTERNET EXPLORER signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	System32: INTERNET INFORMATION SERVICES signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	System32: MICROSOFT IME 2012 signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	System32: WINDOWS DRIVE OPTIMIZER signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	System32: MICROSOFT (R) WINDOWS (R) OPERATING SYSTEM signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	System32: MICROSOFT(R) CONNECTION MANAGER signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	System32: WINDOWS INSTALLER - UNICODE signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	Everyone	ACRORD32.EXE, version 15.16.0.0 and above, in ADOBE ACROBAT READER DC, from O=ADOBE SYSTEMS, INCORPORATED, L=SAN JOSE, S=CALIFORNIA, C=US	Vydavatel	
Povolit	Everyone	System32: MICROSOFT® DRM signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Vydavatel	
Povolit	S-1-5-21-2098876728-...	%OSDRIVE%*	Cesta	
Povolit	BUILTIN\Administrators	(Default Rule) All files	Cesta	
Povolit	Everyone	eDrawingOfficeAutomator.exe, eDrawings.exe, EModelViewer.exe	Hodnota hash souboru	
Povolit	Everyone	Tlac_ciaroveho_kodu.exe	Hodnota hash souboru	
Odepřít	S-1-5-21-2098876728-...	Disable Windows binaries	Hodnota hash souboru	
Povolit	Everyone	Microsoft.Net	Hodnota hash souboru	
Povolit	Everyone	System32: aitagent.exe, aitstatic.exe, pcaui.exe	Hodnota hash souboru	

Obr. 22: Applocker – nastavenia, vlastný zdroj.

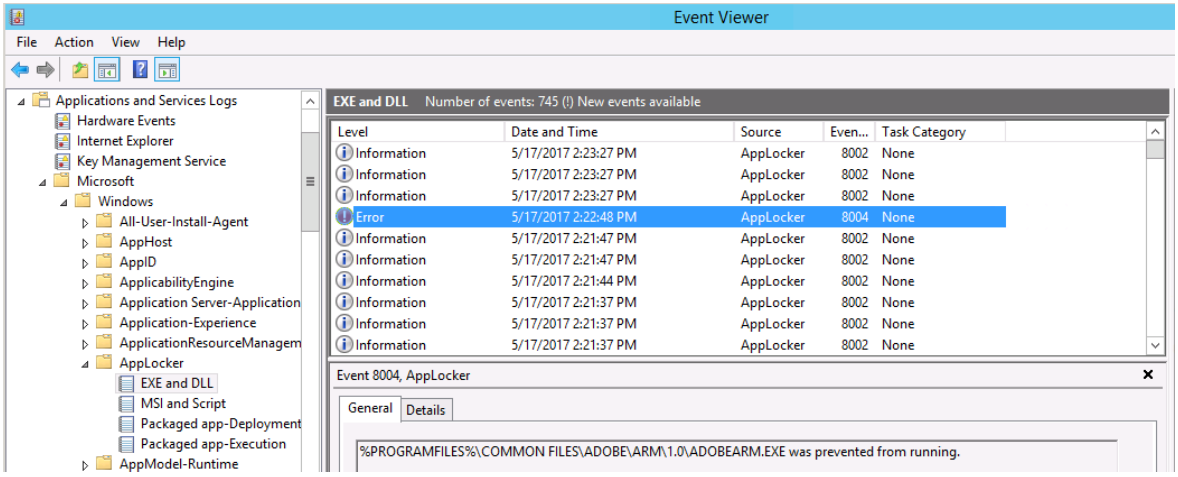
Vyššie uvedené pravidlá pre skupinu Everyone (na základe Vydavateľa), umožňujú spúšťať aj súčasti, ku ktorým by skupina „RDS users“ nemala mať prístup. Tieto komponenty boli preto explicitne zakázané (na základe Hash odtlačku súboru).



Obr. 23: Applocker – Hash pravidlá, vlastný zdroj.

V prípade, aktualizácie niektorej z aplikácií, na ktorú sa vzťahuje Hash pravidlo, je samozrejme ďalšie spustenie danej aplikácie zablokované a je nevyhnutné aplikáciu do skupinovej politiky znovu nadefinovať.

Primárnym nástrojom v prípade riešenia problémov s aplikovaním Applocker pravidiel, je pre administrátora Protokol udalostí (Protokol udalostí a služieb, Applocker skupina).



Obr. 24: Applocker – Protokol udalostí, vlastný zdroj.

9.5 Konfigurácia Tenkého klienta

Pre testovacie účely bol zvolený tenký klient **HP t520 Flexible Series Thin Client** s 32 bitovým operačným systémom Windows Embedded Standard 7E.

Obr. 25: HP t520 Flexible Series Thin Client [41].

Tenký klient vo výrobe bol zapojený do vyhradeného sieťového segmentu a IP konfigurácia sa získava automaticky z DHCP servera.

Pretože štandardná inštalácia operačného systému obsahuje zabudovaný Write Filter (popísaný nižšie), pre pridanie klienta do existujúcej domény bolo nevyhnutné vykonať dodatočné kroky.

Postup pridania do domény:

- Zakázanie Write filtra.
- Pridanie do domény.
- Reštart počítača.
- Povolenie Write filtra.

9.5.1 Write Filter

Je dôležitým komponentom, ktorý je srdcom zabezpečenia tenkého klienta. Jedná sa o dodatočnú vrstvu medzi diskovým úložiskom a operačným systémom. Všetky operácie, ktoré požadujú zápis údajov na disk, musia prejsť týmto filtrom. Ak je filter povolený, čo je štandardné nastavenie, potom sú všetky zápisy na disk uložené dočasne do pamäte. To znamená, že po reštarte systému budú všetky údaje, ktoré sa v pamäti nachádzali, stratené. Ak je filter vypnutý, potom zápis na disk funguje rovnako, ako pri bežnom počítači.

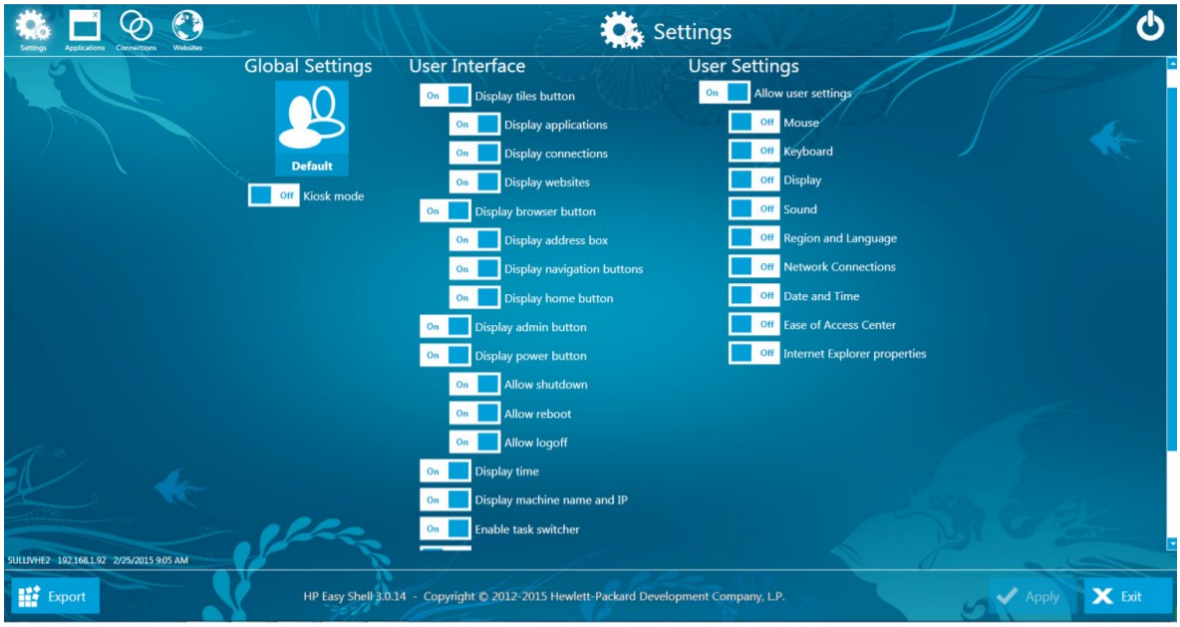
Pri všetkých konfiguračných zmenách preto bolo nevyhnutné postupovať nasledovne:

- Prihlásiť sa ako administrátor.
- Zakázať Write filter na systémovej lište (ikona zmení svoju farbu na červenú).
- Reštartovať tenkého klienta.
- Vykonať potrebné konfiguračné zmeny.
- Povoliť Write filter na systémovej lište (ikona zmení svoju farbu na zelenú).
- Reštartovať tenkého klienta.

9.5.2 HP Easy Shell

Je Windows aplikácia, pomocou ktorej je možné prispôsobiť užívateľské rozhranie na tenkom klientovi. Aplikácia umožňuje zablokovať spúšťanie jednotlivých aplikácií a komponentov systému. Zároveň umožňuje prepnúť užívateľské rozhranie do tzv. Kiosk módu, kde sa užívateľovi hneď pri štarte spúšťa na celú obrazovku iba jedna správcom definovaná aplikácia.

Kombináciou Kiosk módu definovaného cez HP Easy Shell a aplikovaných doménových politík, bol nakonfigurovaný relatívne dobre zabezpečený systém, umožňujúci pracovníkom vo výrobe spúšťať iba aplikácie, ktoré definoval systémový správca.



Obr. 26: HP Easy Shell [42].

9.5.3 Konfigurácia systému BIOS

Na tenkom klientovi boli vykonané tieto konfigurácie:

- Definované heslo pre vstup do BIOS-u (Administrator Password) – bežný užívateľ, ani potenciálny útočník bez znalosti hesla nebude schopný vykonať žiadne zmeny.
- Pevne definované poradie bootovania (Boot Order) – bolo definované iba jedno zariadenie, z ktorého môže daný systém nabehnúť a to vstavaný pevný disk.
- Zakázané nepoužívané porty – Sériový a paralelný.

9.5.4 Dodatočné konfigurácie

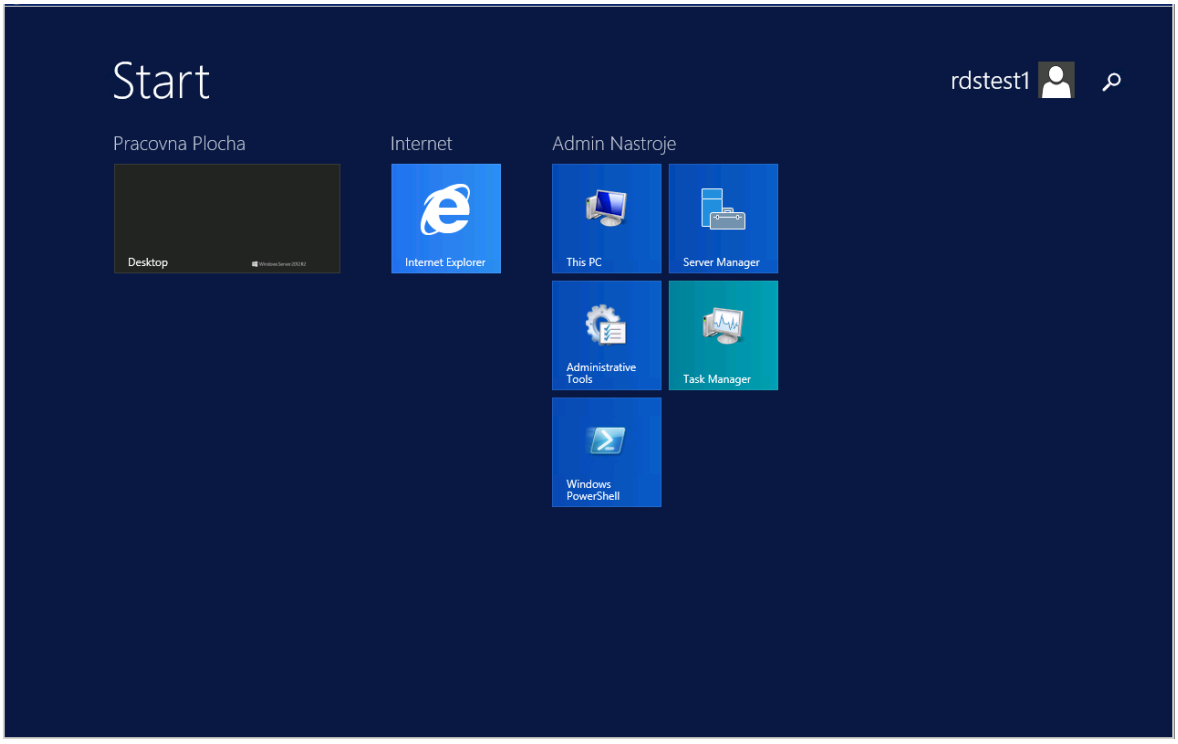
Pre zvýšenie úrovne bezpečnosti a naplnenia všetkých požiadaviek organizácie, boli vykonané nasledovné dodatočné konfiguračné zmeny:

- Zablokovanie prístupu na internet zo sieťového segmentu, kde sa nachádzajú tenkí klienti.
- Zablokovanie USB prenosných diskov a flash medií v registry databáze na tenkom klientovi.
- Obmedzenia v Remote desktop klientovi súvisiace s pripájaním zariadení.

10 TESTOVANIE KONFIGURÁCIE

Cieľom testovania bolo overiť, či sú splnené všetky definované požiadavky a prípadné doladenie zistených chybových stavov. Pre účely testu, bol vytvorený nový doménový užívateľ „rdstest1“. Užívateľ bol štandardne ponechaný v skupine doménových užívateľov a zároveň bol pridaný do skupiny „RDS users“. Pre skupinu „RDS users“ boli definované požadované oprávnenia na súborovom serveri – prístup na čítanie do zložky, kde sú uložené výrobné výkresy.

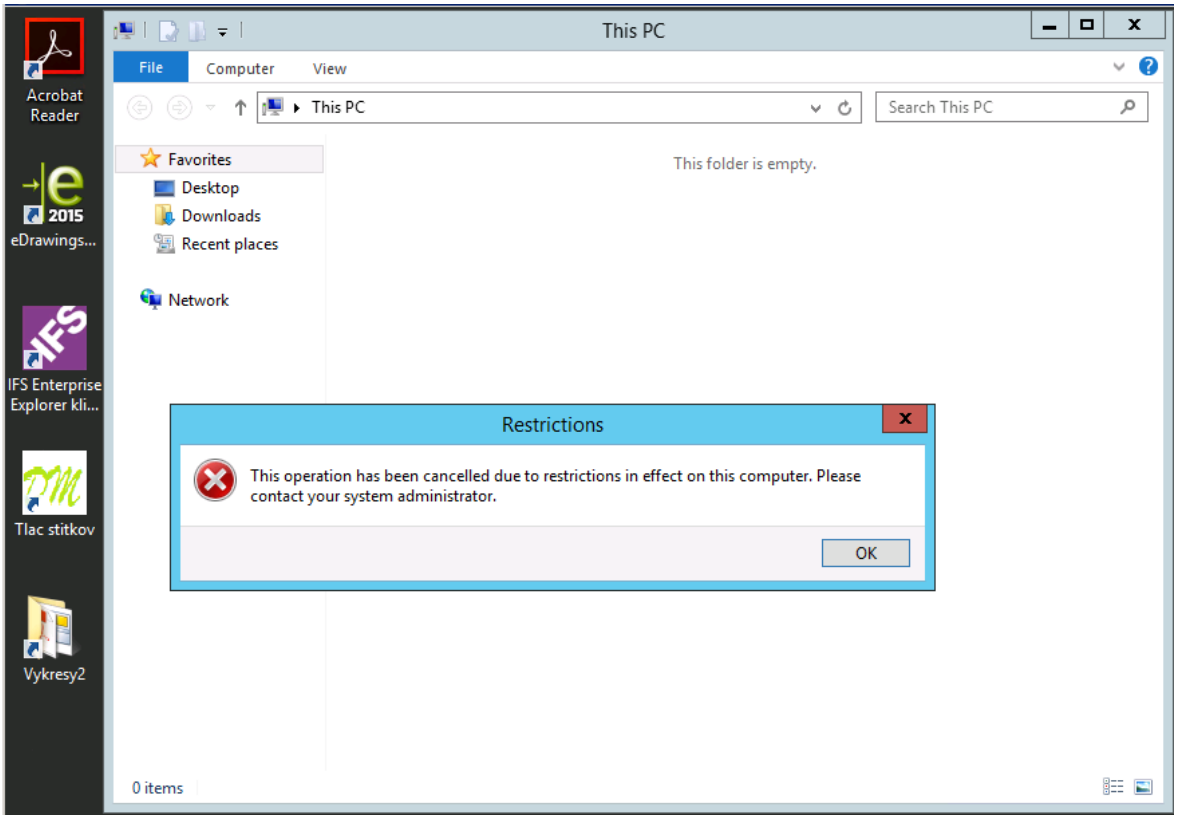
Tenký klient bol nakonfigurovaný tak, že po jeho zapnutí prebehne automatické prihlásenie generického užívateľa a spustí sa Remote desktop klient, kde užívateľ zadáva jeho osobné doménové prihlasovacie meno a heslo. Po úspešnom prihlásení sa užívateľ dostane na vzdialenú plochu RDS servera, kde sa mu zobrazia správcom definované štart menu položky.



Obr. 27: Štart menu položky, vlastný zdroj.

Ako vidno z obrázku nižšie, pri pokuse o zobrazenie lokálnych diskov, sa užívateľovi zobrazilo iba prázdne okno.

Pri pokuse o spustenie blokovanej aplikácie, dostal užívateľ chybovú hlášku: „This operation has been cancelled due to restrictions ...“.



Obr. 28: Pokus o spustenie blokovanej aplikácie, vlastný zdroj.

Pokus o prístup k povoleným aplikáciám prebehol úspešne a užívateľ s nimi vedel plnohodnotne pracovať.

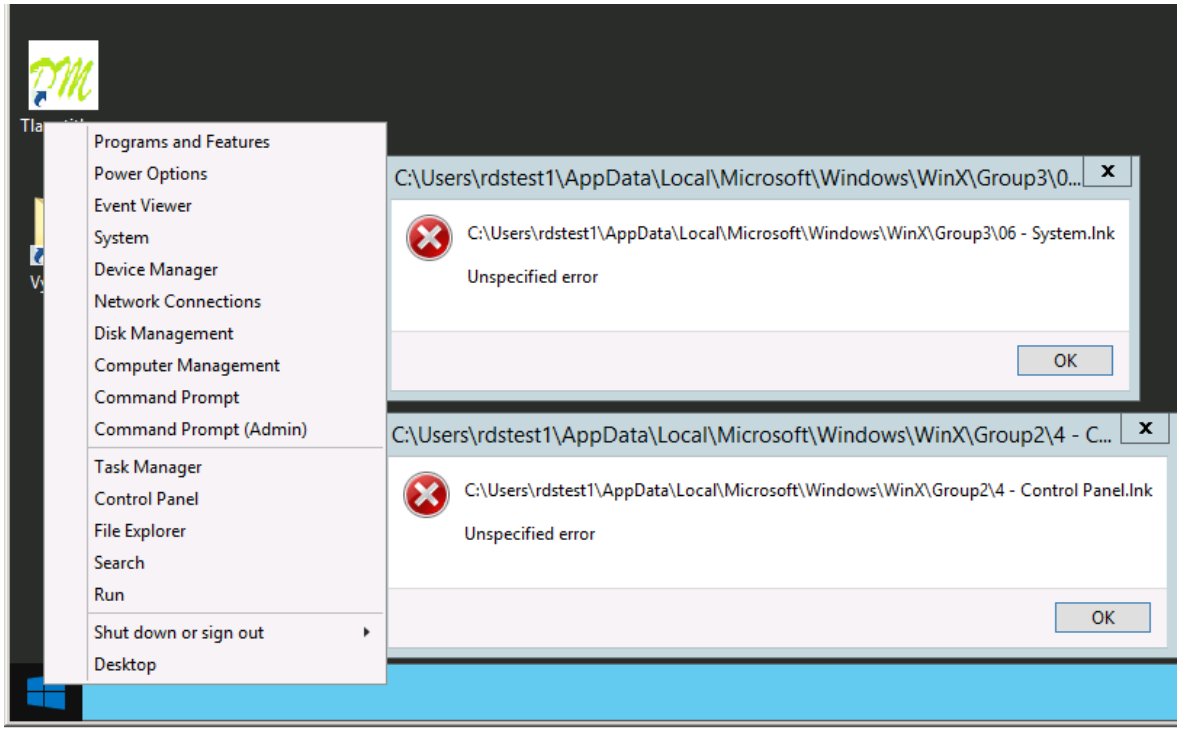
Pokus o zmenu užívateľského rozhrania bol neúspešný, rovnako ako snaha o zápis, alebo modifikáciu dát na zdieľanom sieťovom úložisku.

Jednotlivé položky a záložky kontextových menu boli blokované, čo znamená, že sa užívateľovi nezobrazili jednotlivé záložky, ani vlastnosti pri prehliadaní odkazov na pracovnej ploche.

Rovnako nebolo možné modifikovať systémovú lištu. Pri pokuse o zobrazenie vlastností (pravý klik), nebolo zobrazené kontextové menu.

Užívateľ bol schopný modifikovať štart menu položky, ale jeho zmeny boli po odhlásení sa zo vzdialenej plochy stratené, z dôvodu aplikácie mandatory profilu.

Ak sa užívateľ pokúšal dostať ku komponentom Ovládacích panelov, výsledkom bola ďalšia chybová hláška.



Obr. 29: Pokus o spustenie komponentov Ovládacích panelov, vlastný zdroj.

10.1 Vyhodnotenie testovania

Vyhodnotením prvotnej etapy testovania, bol zoznam počiatočných požiadaviek so stručným popisom riešenia daného problému.

- Zamedziť úniku dát vo výrobe
    - Zamedziť spúšťaniu a inštalácii nepovolených aplikácií na klientskej stanici – **Write filter, BIOS nastavenia, HP Easy shell.**
    - Zamedziť možnosti konfigurácie klientskej stanice bežným užívateľom – **Write filter, HP Easy shell.**
    - Zamedziť používaniu USB prenosných diskov a zariadení – **konfiguračné nastavenia databázy registry na tenkom klientovi.**
    - Minimalizácia úniku firemných dát v prípade odcudzenia počítača vo výrobe – **na tenkého klienta nie je možné uložiť žiadne dáta, preto jeho prípadné odcudzenie nie je pre spoločnosť hrozbou s ohľadom na únik dát.**
- Zníženie poruchovosti počítačov vo výrobe – **tenký klient ako taký, neobsahuje žiadne mechanicky pohyblivé časti a preto je do daného prostredia vhodnejší, ako bežný kancelársky počítač.**
- Zvýšenie bezpečnosti citlivých údajov na súborovom serveri – **nasadenie ACL a rozšíreného auditovania pre dáta vedenia spoločnosti.**
- Jednotná konfigurácia užívateľskej pracovnej plochy – **„RDS settings“ doménová skupinová politika a mandatory užívateľský profil.**
- Centralizovaná a zjednodušená administrácia počítačov a užívateľov – **implementovaná Active Directory infraštruktúra spoločnosti.**
- Zjednodušená správa a aktualizácia definovaných aplikácií – **RDS server a aplikácie na ňom nainštalované.**

ZÁVER

Obľúbeným sloganom v radoch systémových administrátorov je: „Prostredie je alebo bezpečné, alebo použiteľné!“. Pravda je však niekde uprostred. Tak, ako nie je problém logickú bezpečnosť úplne odignorovať, väčšinou nie je veľký problém ani povoliť všetky bezpečnostné prvky. V prvom aj druhom prípade, však spoločnosť veľmi rýchlo zistí, že ich IT infraštruktúra je nepoužiteľná. To, čo je pre správcov výzvou, je navrhnúť a nakonfigurovať prostredie, ktoré spĺňa požadované bezpečnostné, ale zároveň aj funkčne požiadavky.

V svojej práci som sa snažil zamerať na súčasti, ktoré sú jednoducho použiteľné aj v prostredí menšej spoločnosti. Cieľom riešenia preto bolo nielen zvýšenie samotnej bezpečnosti, ale aj jednoduché nasadenie, centralizovaná správa a v neposlednom rade aj zjednodušenie dennej činnosti správcu, zodpovedného za danú infraštruktúru.

Praktická časť začína popisom súčasného stavu fiktívnej spoločnosti. Stručne bola zhrnutá organizačná štruktúra, hardvérové a softvérové vybavenie a sieťová topológia. Prvú časť uzatvára zoznam cieľov a požiadaviek spoločnosti.

Návrhová časť, popisuje jednotlivé konfiguračné nastavenia a princípy fungovania. Súborový server, použitý ako úložisko jednotného, správcom definovaného užívateľského profilu a zároveň miesto, kde sú uchovávané, zabezpečené a auditované zdieľané dokumenty spoločnosti.

Ďalším komponentom je služba vzdialenej plochy. Klienti na pripojenie k serveru využívajú aplikáciu štandardne vstavanú vo svojom operačnom systéme a po pripojení sa na vzdialenú plochu servera, získavajú prístup k vybraným vnútropodnikovým aplikáciám. Týmto spôsobom bolo zabezpečené centralizované riadenie prístupu a zároveň uľahčenie administrácie a správy týchto aplikácií.

V rámci Adresárovej služby bol vytvorený nový doménový testovací užívateľ, globálna skupina a najdôležitejší objekt – skupinová politika „RDS settings“. V politike boli definované všetky obmedzenia aplikované na užívateľa, ktorý pracuje zo serverom vzdialenej plochy. Špeciálnu pozornosť si zaslúži Applocker časť, kde bolo na základe Vydavateľa, odtlačku (Hash) súboru, alebo cesty k danému súboru, povolené alebo naopak zablokované spúšťanie jednotlivých aplikácií, programov aj samotných Windows komponentov..

Predposledná časť sa zaoberá konfiguráciou tenkého klienta HP s operačným systémom Windows 7. Kapitola obsahuje popis pridania klienta do domény a z pohľadu bezpečnosti dôležité konfigurácie komponentov ako sú Write Filter, či BIOS zariadenia.

Praktickú časť uzatvárajú testy konfiguračných nastavení a ich krátke vyhodnotenie. Cieľom testovania bolo overiť, že testovací doménový užívateľ vo výrobe, pripájajúci sa na server vzdialenej plochy, môže využívať iba aplikácie povolené správcom systému a má jednotne definované užívateľské rozhranie, ktoré nemá možnosť modifikovať. Zároveň sa podarilo overiť, že užívateľ nemal možnosť ukladať, alebo presúvať žiadne dáta zo súborového servera priamo na tenkého klienta. Test funkčnosti riešenia sa preto považoval za úspešný a splnil definované ciele.

Oblasti v ktorých vidím možnosti zlepšenia sa týkajú zvýšenia ochrany citlivých údajov spoločnosti:

- Fyzická ochrana dát na serveroch – šifrovanie diskov pomocou Bitlocker aplikácie.
- Ochrana prenosných a flash USB diskov – centralizované nasadenie Bitlocker to Go.
- Zabezpečenie dát v prípade, že opustia vnútropodnikovú sieť – AD RMS.

Častým problémom nielen v menších spoločnostiach sú výdavky na IT. V návrhu je v podstate použitá iba jedna technológia, ktorá si vyžaduje dodatočné náklady v podobe licencií. Jedná sa o služby vzdialenej plochy. Aj to je dôkazom, že nie je dôvod bezpečnosť prostredia postaveného na Microsoft Active Directory infraštruktúre ignorovať. Veď prečo nevyužiť niečo, čo výrobca poskytuje v cene produktu, ktorý už má spoločnosť zakúpený a denne ho využíva?

ZOZNAM POUŽITEJ LITERATÚRY

[1] *Windows Server 2012 R2 Products and Editions Comparison* [online]. [cit. 2017-04-20]. Dostupné z: https://www.microsoft.com/en-us/download/confirmation.aspx?id=41703

[2] VHD Soubor - Wikipedie: VHD Soubor. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2017-04-20]. Dostupné z: https://cs.wikipedia.org/wiki/VHD_soubor

[3] Co je nového ve Vzdálené ploše ve Windows Serveru. *Microsoft TechNet* [online]. Microsoft, 2014 [cit. 2017-04-20]. Dostupné z: https://technet.microsoft.com/cs-cz/library/dn283323(v=ws.11).aspx#BKMK_Admin]

[4] DESMOND, Brian, Joe RICHARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. *Active Directory: Designing, Deploying, and Running Active Directory*. 5'th. United States of America: O'Reilly Media, 2013. ISBN 978-1-449-32002-7.

[5] *Windows Server 2012 R2 Licensing Datasheet* [online]. Microsoft [cit. 2017-04-20]. Dostupné z: http://download.microsoft.com/download/F/3/9/F39124F7-0177-463C-8A08-582463F96C9D/Windows_Server_2012_R2_Licensing_Datasheet.pdf

[6] System Requirements and Installation Information for Windows Server 2012 R2. *Microsoft TechNet* [online]. Microsoft, 2015 [cit. 2017-04-20]. Dostupné z: https://technet.microsoft.com/en-us/library/dn303418(v=ws.11).aspx

[7] *Windows Server 2008 R2: Active Directory* [online]. Microsoft [cit. 2017-04-22]. Dostupné z: https://www.microsoft.com/slovakia/windowsserver2008/active-directory.aspx

[8] Directory Partitions. *Microsoft TechNet* [online]. Microsoft [cit. 2017-04-22]. Dostupné z: https://technet.microsoft.com/en-us/library/cc961591.aspx

[9] What Is the Global Catalog?: Active Directory. *Microsoft TechNet* [online]. Microsoft, 2014 [cit. 2017-04-22]. Dostupné z: https://technet.microsoft.com/en-us/library/cc728188(v=ws.10).aspx

[10] Active Directory Object attributes. *Active Directory Object attributes and their purpose.* [online]. [cit. 2017-04-22]. Dostupné z: http://www.windows-active-directory.com/active-directory-object-attributes.html

[11] BUMBÁL, Lukáš. *Riešenie problémov s užívateľskými profily v doméne UCN* [online]. Brno, 2011 [cit. 2017-04-22]. Dostupné z: https://is.muni.cz/th/325035/fi_b/Lukas_Bumbal_325035_Bakalarska_praca.pdf. Bakalárska práca. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Mgr. Jakub Dobrovolný.

[12] Logical Structure and Areas of Active Directory. *Active Directory Structural Areas* [online]. [cit. 2017-04-22]. Dostupné z: http://www.distributednetworks.com/active-directory-administration/module2/activeDirectory-logical-structure.php

[13] What Are Domains and Forests? : Active Directory. *Microsoft TechNet* [online]. Microsoft, 2014 [cit. 2017-04-22]. Dostupné z: https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx

[14] Principy vztahů důvěryhodnosti. *Microsoft TechNet* [online]. Microsoft, 2012 [cit. 2017-04-23]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc731335(v=ws.11).aspx

[15] *FSMO Roles – In detail* [online]. [cit. 2017-04-22]. Dostupné z: http://www.windows-active-directory.com/active-directory-fsmo-roles-details.html

[16] *Zobrazenie a prenos rolí FSMO v systéme Windows Server 2003* [online]. Microsoft, 2008 [cit. 2017-04-22]. Dostupné z: https://support.microsoft.com/sk-sk/help/324801/how-to-view-and-transfer-fsmo-roles-in-windows-server-2003

[17] PDC Emulator FSMO Role. *Microsoft Developer Network* [online]. Microsoft [cit. 2017-04-22]. Dostupné z: https://msdn.microsoft.com/en-us/library/cc223752.aspx

[18] RID Master FSMO Role. *Microsoft Developer Network* [online]. Microsoft [cit. 2017-04-22]. Dostupné z: https://msdn.microsoft.com/en-us/library/cc223751.aspx

[19] Organizational Units. *Microsoft TechNet* [online]. Microsoft [cit. 2017-04-22]. Dostupné z: https://technet.microsoft.com/en-us/library/cc978003.aspx

[20] Designing OU Structures That Work: Choosing The Best Model. *Microsoft TechNet* [online]. Microsoft, 2008 [cit. 2017-04-23]. Dostupné z: https://technet.microsoft.com/en-us/library/2008.05.oudesign.aspx

[21] Principy skupin. *Microsoft TechNet* [online]. Microsoft, 2009 [cit. 2017-04-23]. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd861330(v=ws.11).aspx

[22] Active Directory Design. *Microsoft Developer Network* [online]. Microsoft, 2001 [cit. 2017-04-23]. Dostupné z: https://msdn.microsoft.com/en-us/library/bb742592.aspx

[23] KOŘÍNEK, Ondřej. *Implementace Active Directory Domain Services* [online]. Zlín, 2010 [cit. 2017-04-26]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/13138/ko%C5%99%C3%ADnek_2010_dp.pdf?sequence=1. Diplomová Práce. UTB ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Doc. Ing. Martin Sysel, Ph.D.

[24] *Active Directory Objects and Attributes* [online]. [cit. 2017-04-26]. Dostupné z: http://www.windows-active-directory.com/active-directory-objects.html

[25] Group Policy Basics – Part 2: Understanding Which GPOs to Apply - Midnight Musings of a Technical TAM. *Microsoft TechNet* [online]. Microsoft, 2012 [cit. 2017-04-26]. Dostupné z: https://blogs.technet.microsoft.com/musings_of_a_technical_tam/2012/02/15/group-policy-basics-part-2-understanding-which-gpos-to-apply/

[26] *Group Policy Preferences: báječný doplněk vašich politik!* [online]. Daquas [cit. 2017-04-26]. Dostupné z: http://www.daquas.cz/articles/335-group-policy-preferences-bajecny-doplnek-vasich-politik

[27] Group Policy for Beginners. *Microsoft TechNet* [online]. Microsoft, 2011 [cit. 2017-04-26]. Dostupné z: https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx

[28] FRANKLIN SMITH, Randy. *Controlling Group Policy, Part 1: Group Policy content from IT PRO* [online]. 2000 [cit. 2017-04-26]. Dostupné z: http://windowsitpro.com/group-policy/controlling-group-policy-part-1

[29] Administer AppLocker. *Microsoft TechNet* [online]. Microsoft, 2012 [cit. 2017-04-26]. Dostupné z: https://technet.microsoft.com/en-us/library/hh994629(v=ws.11).aspx

[30] Delegované úkoly. *Microsoft TechNet* [online]. Microsoft, 2008 [cit. 2017-04-27]. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd145442(v=ws.11).aspx

[31] Pokročilé zásady auditu zabezpečení. *Microsoft TechNet* [online]. Microsoft, 2016 [cit. 2017-04-27]. Dostupné z: https://technet.microsoft.com/cs-cz/library/dn319056(v=ws.11).aspx

[32] Vynútenie zabezpečenia a zásad. *Windows Server 2008 R2* [online]. Microsoft [cit. 2017-04-27]. Dostupné z: https://www.microsoft.com/slovakia/windowsserver2008/security-policy.aspx

[33] Identita a prístup. *Windows Server 2008 R2* [online]. Microsoft [cit. 2017-04-27]. Dostupné z: https://www.microsoft.com/slovakia/windowsserver2008/identity-access.aspx

[34] Přehled služby Vzdálená plocha. *Microsoft TechNet* [online]. Microsoft [cit. 2017-04-27]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc725560(v=ws.11).aspx

[35] CHOU, Yung. *Remote Desktop Services (RDS) Architecture Explained: Yung Chou on Hybrid Cloud* [online]. Microsoft, 2010 [cit. 2017-04-27]. Dostupné z: https://blogs.technet.microsoft.com/yungchou/2010/01/04/remote-desktop-services-rds-architecture-explained/

[36] Systém DNS. *Microsoft TechNet* [online]. Microsoft [cit. 2017-04-27]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc730921(v=ws.11).aspx

[37] Přehled služby DHCP. *Microsoft TechNet* [online]. Microsoft [cit. 2017-04-27]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc731166(v=ws.11).aspx

[38] PLZÁK, Jan. *Konfigurace serveru jako řadiče domény pro malou podnikovou síť* [online]. Zlín, 2012 [cit. 2017-04-27]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/22798/plz%C3%A1k_2012_bp.pdf?sequence=1. Bakalářská práce. UTB ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Ing. Jiří Korbel, Ph.D.

[39] VALÁŠEK, Martin. *Výhody tenkých klientov zatiaľ zákazníkov neoslovili: Technológie|Trend* [online]. 2004 [cit. 2017-04-27]. Dostupné z: https://www.etrend.sk/technologie/vyhody-tenkych-klientov-zatial-zakaznikov-neoslovili.html

[40] *Wyse 7000 Series Thin Clients | High-Performance Virtual Desktop: Dell, United States* [online]. [cit. 2017-04-27]. Dostupné z: http://www.dell.com/us/business/p/wyse-z-class/pd

[41] *Troubleshooting Guide: HP t520 Flexible Thin Client* [online]. HEWLETT PACKARD. Hewlett-Packard Development Company, 2014 [cit. 2017-05-20]. Dostupné z: https://content.etilize.com/User-Manual/1035698196.pdf

[42] *Technical white paper: HP Easy Shell* [online]. HEWLETT PACKARD. Hewlett-Packard Development Company, 2015 [cit. 2017-05-20]. Dostupné z: http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA5-7322ENW

[43] ANDERSON, Christa a Kristin L. GRIFFIN. *Windows Server 2008 R2 Remote Desktop Services Resource Kit*. Redmond, Washington: Microsoft Press, 2010. ISBN 9780735627376.

[44] MOSKOWITZ, Jeremy. *Group Policy: Fundamentals, Security, and the Managed Desktop*. 3'rd. Indianapolis, Indiana: John Wiley & Sons, 2015. ISBN 978-1-119-03558-9.

[45] WRIGHT, Byron a Brian SVIDERGOL. *Virtualizing Desktops & Apps with Windows Server 2012 R2 Inside Out*. 1'st. Redmond, Washington: Microsoft Press, 2015. ISBN 978-0-7356-9721-8.

[46] SMITH, Russell. *Least Privilege Security for Windows 7, Vista and XP*. 1'st. Olton, Birmingham: Packt Publishing, 2010. ISBN 978-1-849680-04-2.

ZOZNAM POUŽITÝCH SKRATIEK

ACL	Access Control List
AD	Active Directory
AD DS	Active Directory Domain Services
AD RMS	Active Directory Rights Management Services
BIOS	Basic Input Output System
BYOD	Bring Your Own Device
CA	Certification Authority
CAL	Client Access License
CD	Compact Disc
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Naming System
DVD	Digital Versatile Disc
EFS	Encrypted File System
FSMO	Flexible Single Master Operations
GPO	Group Policy Object
GUID	Globally Unique Identifier
HP	Hewlett Packard
HW	Hardware
IIS	Internet Information Services
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
PKI	Public key Infrastructure
IT	Information Technology
MS	Microsoft
NTFS	New Technology File System
OS	Operating System
OU	Organization Unit
PC	Personal Computer
PKI	Public Key Infrastructure
RD	Remote Desktop

RDS	Remote Desktop Services
RSAT	Remote Server Administration Tools
SID	Security Identifier
SSO	Single Sign on
TCP/IP	Transmission Control Protocol/Internet Protocol
TPM	Trusted Platform Module
USB	Universal Serial Bus
VHD	Virtual Hard Drive
WINS	Windows Internet Naming Service
WSUS	Windows Server Update Services

ZOZNAM OBRÁZKOV

Obr. 1: Logická štruktúra Adresárovej služby (doména, strom a les) [12]. 17
Obr. 2: Doména, strom, les a vzťahy dôvery [13].....19
Obr. 3: Model kombinovanej hierarchie organizačných jednotiek, vlastný zdroj. 21
Obr. 4: Rozsah skupín [22].....23
Obr. 5: Model použitia skupín – AGDLP [22].....23
Obr. 6: Editor správy zásad skupiny (Group Policy Management Editor), vlastný zdroj. 27
Obr. 7: Spôsob aplikovania politík [28].....28
Obr. 8: Applocker skupinová politika, vlastný zdroj. 29
Obr. 9: Súčasti RDS infraštruktúry [35]. 35
Obr. 10: Tenký Klient – Dell Wyse 7000 [40].....40
Obr. 11: Organizačná štruktúra spoločnosti, vlastný zdroj. 42
Obr. 12: Komponenty HW infraštruktúry, vlastný zdroj.....43
Obr. 13: Sieťová topológia, vlastný zdroj. 44
Obr. 14: Role RDS, vlastný zdroj. 47
Obr. 15: Režim spracovania duplicitných zásad skupiny užívateľa, vlastný zdroj.....48
Obr. 16: Konfigurácia skupín s obmedzeným členstvom, vlastný zdroj. 49
Obr. 17: Konfigurácia profilu, vlastný zdroj. 50
Obr. 18: Ponuka štart a Hlavný panel – nastavenia, vlastný zdroj.....50
Obr. 19: Ovládacie panely – nastavenia, vlastný zdroj.....51
Obr. 20: Pracovná plocha – nastavenia, vlastný zdroj. 52
Obr. 21: Prieskumník systému Windows a položky Systém - nastavenia, vlastný zdroj. 52
Obr. 22: Applocker – nastavenia, vlastný zdroj. 53
Obr. 23: Applocker – Hash pravidlá, vlastný zdroj. 53
Obr. 24: Applocker – Protokol udalostí, vlastný zdroj. 54
Obr. 25: HP t520 Flexible Series Thin Client [41]. 55
Obr. 26: HP Easy Shell [42]. 57
Obr. 27: Štart menu položky, vlastný zdroj.....58
Obr. 28: Pokus o spustenie blokovanej aplikácie, vlastný zdroj. 59
Obr. 29: Pokus o spustenie komponentov Ovládacích panelov, vlastný zdroj. 60

ZOZNAM TABULIEK

Tab. 1: Porovnanie edícií Windows Server 2012 R2 [1]. 12
Tab. 2: Potrebné množstvo licencií pre jednotlivé nasadenia [5]. 14
Tab. 3: Minimálne hardvérové požiadavky [6]. 14
Tab. 4: Zoznam serverov a rolí, vlastný zdroj. 44
Tab. 5: RDS server – použité licencie, vlastný zdroj. 47
Tab. 6: RDS server – hardvérové parametre, vlastný zdroj. 48