Windows - sprava systemu I

Instalacia

- high, little a zero touch
- dotazy instalatoru mozme automatizovat pomocou answer file - unatted.xml
- little touch len spusti instalaciu, instalacia prebehne bez obsluhy
- zero boot zo siete, bez obsluhy
- image based instalacia - thick (s aplikaciami uz naistalovanymi), thin (len os) a hybrid (len os ale script niastaluje aplikacie po instalacii os)
- exstuju aj logy pri instalacii ich umiestnenie je ale imba (podla druhu logu je umiestnenie vzdy inde)

Migracia

- kompatibilita aplikacii - Application Compatibility Toolkit (ACT)
- kompatibilita HW - Assessment and Planning Toolking (MAP)

Windows edicie a licencie

- retail, OEM, Volume a legalizacna licencia
- overenie Volume licencie - MAK (Multiple activation key), len jedne kluc overuje sa cez server MS. 2. KMS (Key management service) overuje a cez lokalny server, ktory je vsak napojeny na MS server. KMS vyzaduje pravidelne pripojenie na KMS server.
- starter, home basic, home premium, proffesional, enterprise, ultimate

Startup

- Sousti sa pc - self test (post)
- bios hlada bootovacie zariadenie - z neho precita MBR (ak je to disk) a tam najde active bootable partition. Spusti kod v tej partitione (boot sector code) konkretne u windows spusti Bootmgr (boot manager)
- boot manager precita BCD (boot configuration data) a ak obsahuje viac ako jeden zaznam tak ich zobrazi a umozni zvolit is os
- taktiez bootmgr obsahuje advanced boot options (safe mod a tak) a memory diagnostics
- f8 hned po post - safe mod, last known good configuration, enable boot logging, enable vga mode, disable automatic restart on system failure
- windows recovery enviroment - poskodene mbr bootrec /fixmbr, chyba v boot sectore /fixboot a chyba bcd /scannos a /rebuildbcd
- chyba disku - chkdsk | System restore - obnova registrov zo zalohy (kazdych 12 hodin) Windows\System32\Config\RegBack
- bootlog je mozne spustit aj v msconfig

Windows - sprava systemu I

Kernel loading faza

- spusti sa Windows Boot Loader a ten nahraje ntoskrnl.exe a hal.dll
- nasledne WBL nahraje konfiguraciu systemu z registrov HKLM\SYSTEM\CurrentControlSet (Windows\System32\Config\System) a spusti vsetky sluzby a ovladade nutne k startu
- WBL preda kontrolu ntoskrnl.exe a ten vytvori klon Control Set
- system zamrzne pri splash screen - väcsinou chybny ovladac, moze pomoct last known good configuration

Logon faza

- spusti sa podsystem sluzieb (services.exe) a ten spusti sluzby ktore maju nastavene autoload v HKLM\SYSTEM\CurrentControlSet\Services*ServiceName*
- spusti sa local Security Authority (LSA) procesess lsass.exe
- ak je pc v domene caka na stisk ctrl+alt+delete
- po prihlasenie nastavi ConstrolSer hodnotu na LastKnownGood
- system prestane reagovat, chybna sluzba alebo aplikacia ktora sa spusti hned po starte systemu

Register

- Kluc - zlozka, Zaznam (entry) - nachadza sa v kluci, sklada sa z mena, typu a hodnoty
- Podkluce HKEY_LOCAL_MACHINE - BCD, hardware, Security Account Manager - SAM informacie o uzivateloch a skuspinach napr hesla, security - bezpecnostne politiky, software - nastavenie programov (globalne), system - nastavenie zaraiadeni a sluzieb
- v HKLM/SYSTEM/select su zanamy Current, Default, Failed a LastKnownGood, samotne controlsety su ulozene v HKLM/SYSTEM/ControlSet00x x je 1 a 2 a currentControlSet ktory len ukazuje na 1 alebo 2, a clone ktory nie je po prihlaseni dostupny
- HKEY_CURRENT_USER - data o aktualne prihlaeneho uzivatela
- HKEY_USERS - uklada informacie o vsetkych uzivateloch
- HKEY_CLASSES_ROOT - link do HKLM/software
- HKEY_CURRENT_CONFIG - informacie o aktuaonom HW link do HKLM/system/CurrentControlSet/hardwareProfiles/Current
- uprava - regedit.exe v system32 alebo v cmd reg.exe
- umiestnenie: windows/system32/config
- zakladne subory v system32/config: Default, Sam, Security, Software, System - bez pripony
- registre current user su ulozene v Users/"UserName"/ntuser.dat

Windows - sprava systemu I

Disk

- simple volume - jedna partition, multipartition volume - viac ako jeden
- volume - logicka uroven, partition - fyzicka
- rozdelenie disku je popisane v GPT alebo v MBR
- GPT - u EFI systemov - dnes uz sa predavaju UEFI dosky od asusu a msi pre sandy bridge procesory od intelu
- MBR
    - informacie o rozdeleni su v partition table
    - je mozne ho previest na dynamic disk bet straty dat
    - tri druhy odielov: primarny, exteneded a logicky
    - primary max 4, ak je ak extened tak 3
    - extened sluzi ako obal pre logicke odiely ktorych moze byt neobmedzeny pocet.
- kazdej jednotke mozem priradit jedno pismeno a viacero ciest

Dynamic disk

- konverzia z dynamic na basic neuchovava data
- kazdy disk si uchovava informacie o vsetkych dynamickych diskoch v pc a to na konci disku v poslednom 1 MB (LDM)
- druhy dynamickych diskov
    - Simple Volume - diskove miesto z jedneho disku (odiely nemusia naväzovat)
    - Spanned Volume - z dvoch alebo viac diskov (az 32), miesto sa zaplnuje postupne, ked sa zaplni prvy ide sa na druhy. Ak zlyha jeden disk vsetko je prec
    - Stripped volume - softwarovy raid 0, 2-32 diskov, odiely rovnakej velkosti, data deli na 64KB casti a tie zapisuje na viac diskov zaroven, nejde rozsirovat iba zalohovat
    - Mirror volume - raid 1
    - raid 5 nie je vo win7 podporovany (v starsich asi bol)

Stavy diskov v disk management

- Online - ok
- Online (errors) - u dyn. diskov detekovana chyba I/O. Ak nam to nevadi tak dat "Reactivate"
- offiline or missing - u dyn. diskov, ak je HW ok treba dat "Rescan"
- Foreign - u dyn. diskov - disk z ineho pc treba ho importovat
- Unredable - zkusit rescan alebo restart
- unrecognized a no media (u cd mechaniky napr)

Disk 2

- windows podporuje CDFS, UDF, FAT12, FAT16, FAT32, exFat a NTFS
- defragmentacia - default automaticky v stredu 01:00
- nedefregmentuju sa segmenty vúcsie ako 64MB
- win7 rozpozna ssd disk a nedefragmentuje ho, vista ssd defragmetuje co je nezmysel pretoze pristupovu dobu ma konstatnu a taktiez kazdym pristupom sa mu znizuje zivotnost
- superfetch monituruje aplikacie snazi sa predvidat puzitie dat a nacita ich v predstihu do pamäte
- readyBoost vyuzitie flash disku ako cache medzi diskom a ram, pri win7 a ssd disku sa RB nepouziva u visty ano
- sparava diskov v cmd DISKPART v MMC je to sprava diskov, cmd DEFRAG

Skupiny a domeny

- pocitace v sieti mozu byt clenmi skupiny alebo domeny
- rozdiel je v sposobe spravy prostriedkov a zdrojov na sieti
- pocitace v domecej sieti su väscinou sucastou domacej alebo pracovnej skupiny, pocitace na pracovisku su sucastou domeny

Domanaca skupina

- spojenie pocitacov, ktore su automaticky nastavene na zdielanie suborov (hudba, obrazky....), tlaciarni a streamovania medii
- vsetky pc musia byt v rovnakej podsieti
- skupina je chranena heslom, ktore je pri pripojeni do skupina treba zadat (len prvykrat)
- neumoznuje centralnu spravu, podrobne nastavenie opravneni

Pracovna skupina

- vsetky pc su rovnocenne, ziadny nema kontrolu nad inym
- kazdy pc ma sadu vladstnych uctov a skupin
- vsetky pc v jednej podsieti

Domena

- jeden alebo viac pc su servery, pomocou nich spravci riadia zabezpecenia a opravnenia
- ucet v domene sa moze prihlasit na vsetky pc za predpokladuze na to je opravenenie

Windows - sprava systemu I

Prihlasovanie

- domenovy ucet je ulozeny v active directory
- lokalny ucet je ulozeny v Security Accounts Manager (SAM) dazabazi na kazdom pc
- uzivatel sa prihlasi pomocou udajaou (alebo cip karty...) -> dojde k porovnaniu udajov oproti SAM a ak su udaje ok vytvori sa access token
- access token obsahuje informacie o identite uzivatela (SID), clenstvi v skupinach a opravneniach
- SID - identifikuje entity v systeme, uzivatelia pouzivaju mena ale system SID. Pri instalacii sa vytvori SID pocitaca. Vsetky uzivatelske SID su potom zalozene na tomto SID. Ziadny SID sa neopakuje.

Uzivatelsky ucet

- prihlasovacie meno - logon name - sklada sa z dvoch casti, mena uctu a domeny v ktorej je ulozeny. Ucet pc je Keksik-pc a ucet je Keksik tak tvar je Keksik-pc\Keksik. ak je pc clenom domeny NTFI.FI.MUNI.CZ a ucet xmoroz je ulozeny v active directory tak NTFI\xmoroz alebo xmoroz@NTFI.FI.MUNI.CZ
- build-in ucty
    - Administrator - neda sa zmazat a ani odobrat zo skupiny Administrators. V safe mode sa da pouzit aj ked je disabled
    - Guest - default je deaktivovany, neda sa zmazat je clen skupiny Guests
    - Local System - plny pristup k systemu
    - Local Service - rovnaka uroven ako Users
    - Network Service - viac ako service ale menej ako system, pristupuje k sieti pod uctom pocitaca
- windows neumoznuje vnorovanie skupin
- built-in skupiny
    - Administrators - full pristup
    - Backup Operators - mozu zalohovat a obnovaovat subory. Defaultne nie je nikto clenom
    - Guests - min pristup
    - Network Configuration Operators - sprava nastavenia siete
    - Power Users - rozsirene prava, napr vytvaranie uctov a skupin. vo win7 su koli spätnej skompatitbilite
    - Remote Desktop Users - mozu sa pripojit cez siet
    - Users - obmedzeny pristp
    - a dalsie
- specialne skupiny
    - Everyone, Authenticated Users - vsetci autentizovany, Creator Owner, Network - vsetci pripojeny cez siet, Interactive - prave pripojeny

Ucty dodatok

- Permissions (opravnenia) prideluju sa objektom - pristup k zloskam...
- Rights (prava) - pridaluju sa uctu ako sucast bezpecnostnych nastaveni (Security Policy Settings)
- Prava hovoria kto moze robit akcie ktore ovlivnia cely system
- nastroje na spravu, GUI: control panel -user accounts, snap-in Users and Groups v mmc, CMD: net user a net localgroup
- polozky v user accounts - manage your credentials - ulozene hesla, create password reset disk,
- existuju aj well known built-in SIDy napr. Creator owner SID: S-1-3-0, priklad uzivatelskeho SID: S-1-5-21-1554409211-3092155047-418224256-1001, SID sa da najst pomocou regedit v HKEY_USERS
- pri premenovani uctu sa SID nemeni
- locked ucet - system lockne ucet pokial prekroci hranicu zlych prihlaseni
- login a full name uctu su dve rozdielne veci, login je to co je vidiet vo vypise
- spustit program ako iny user - v cmd RUNAS [runas /user:admin notepad], /savecred ulozi heslo do credentials takze sa na neho uz druhykrat nebude dotazovat, GUI - RMB + shift -> run as different user
- lokalne skupiny sa do seba nedaju vnorovat, build-in specialne skupiny ano. Tj. do lokalnej skupiny mozem vlozit skupinu everyone, ale nie administrators.

Atrbibuty suborov a priecinkov

- Read-only - nemozno zmenit ani zmazat
- Hidden
- Archive - subor ktory nebol v blizkej dobe zalohovany. Zalohovaci program oznaci pri zalohovani subor ako archivovany. Ked s asubor zmeni, priznak sa zmaze.
- Compressed
- Encrypted
- System

NTFS opravnenia

- opravnenie udelujeme skupinam alebo jednotlivym userom
- opravnenia moze menit owner a kazdy s opravnenim change permissions
- v systeme je to realizovane pomocu Acces Control List (ACL) pre kazdu slozku a subor
- hodnoty opravnenia Allow, Deny alebo je nedefinovane (nie je pristup, ale nie je explicitne zakazane ako Deny)
- zakladne opravnenia a specialne opravnenia - zakladne sa skladaju zo specialnych

Zakladne opravnenia pre zlozky

- Read, Write, Modify - mozu menit, ale nemozu vytvarat, mozu mazat.
- List Folder Contents
- Read & Excecute - + mozu spustat aplikacie v zlozke
- Full Control

Zakladne opravnenia pre subory

- Read, Write, Read & Execute, Modify - w + r&e, Full Control

Vyhodnocovanie opravneni

- default dedia zlozky a subory opravnenia z nadradenej zlozky, dedenie sa da vypnut
- dve druhy opravneni - explicitne a zdedene. Explicitne su aplikovane priamo na konkreny objekt, zdenene na rodicovsky objekt
- vyhodnocovanie
    1. explicitny Deny
    2. explicinty Allow
    3. zdedeny Deny
    4. zdedeny Allow
- vysledne opravnenie je sucet vsetkych uzivatelskych opravneni + vsektych skupin ktorych je clenom. Explicitny deny ma vzdy prednost. Explicitne allow ma prednost pred zdedenym deny.
- ak mam pristup k suboru ale nie do zlozky kde je umiestneny, mozem sa k nemu dostat ak mam na slozke opravnenie traverse folder a poznam cestu k suboru.
- kazdy subor a zlozka ma vlastnika, vlastnik moze vzdy meni opravnenia. Od Vista+ existuje skupina OWNER RIGHTS pomocou ktorej mozeme nastavovat opravnenia vlastnika. Vyuziva sa pri diskovych kvotach.
- vlastnictvo mozeme prevziat s PRAVOM take ownership of files or toher objects (default administrators), s PRAVOM restore files and directories (default administrators a backup operators) alebo pomocou OPRAVNENIA take ownership
- rozsah opravneni pre priecinky je mozme specifikovat pomocou volieb: this folder only, this folder, subfolder and files, files only.....
- pri kopirovani sa vytvara novy objekt, ten dedi opravnenia od rodica, pri presuvani sa opravnenia zachovavaju, pri presuvavani do inej NTFS jednotky a opravenia dedia od rodica. Vo vsetkych 3 pripadoch sa uzivatel ktory vykonaval presun stane novym vlastnikom

Zdielanie

- zdielane zlozky: v xp Shared Documents, vo Vista+ Public (skupina interactive moze menit cokolvek), Defaultne zdielane len lokalne
- moznosti zdielania
    - Public Folder Sharing - aktivuje zdielanie zlozky Public cez siet
    - File and Printer Sharing - aktivuje moznost zdielania pre ostatne zlozky
    - Password Protected Sharing - ak je ON je vyzadovane prihlasenei s heslom, ak je OFF uzivatelia mozu cez siet pristup aj pomocou uctu Guest
- vytvorit zdielanie mozu len Administrators, CMD prikaz net share
- zdielanei sa da aktivovat len nad zlozkou (vynimka je zdielanie vo vnutri uzivatelskeho profilu)
- opravnenia sa vztahuju len na pristup cez siet, najprv sa vyhodnocuju opravnenia zdielania a potom NTFS opravnenia.
- Opravnenia: Read, Change, Full Control - r + ch + menit opravnenia, take ownership
- default je Everyone: Read
- pri premenovani alebo presunuti sa zdielanie rusi, nekopiruje sa s kopirovanim zlozky
- defaultne su zdielane niektore zlozky pre administrativne ucely - C$, D$, E$, Admin$ (%systemroot%), Print$ (system32/spool/drivers - ovladace tlaciarni). Nefunguju od Vista+ ak je pc clenom pracovnej skupiny

Profily

- Local - ulozeny lokalne.
- Roaming - ulozeny na servery, po prihaseni sa stiahne. Defaultne ostava po prihlaseni profil ulozeny v pc, aby sa nabuduce nestahoval cely. Cim väcsa je velkost profilu tym dlhsie je prihlasovanie. Ked sa prekroci diskova kvota na win7 sa uzivatel odhlasi ale zmeny sa neulozia. Vytvorenie roaming uctu = vytvorenie zdielanej zlozky a zmena cesty k profilu v nastaveniach uctu. Na server sa data nahravaju pri odhlasovani, ak je sucasne ucet prihlaseny na viac pc, tak kazde odhlasenie prepisuje profil. Nahrava sa len ta cast profilu ktora sa zmenila, tj. ak sme menili vzdy ine polozky ku kolizii nedojde. Inak vzdy plati ze posledne odhlasenie prepise predchadzajuce.
- Mandatory - rovnaky ako predchadzajuce, ale neukladaju sa zmeny. Moze byt local aj roaming pomocou premenovania ntser.dat na ntuser.man + prislusne NTFS opravnenia. Super-Mandatory - len vo win7, nazov slozky s profilom ma koncovku .man. Narozdiel od mandatory sa uzivatel neprihlasi ak sa profil nepodari stiahnut.
- Problem velkej velkosti roaming profilu mozme riesit pomocou presmerovania zloziek, kde urcite zlozky mozu byt presmerovane do zdielanej zlozky na serveri.

Profily v XP

- Built-in profily - Default User - vzor pre nove profily, All Users - nastavenia plantne pre vsetkych prihlasenych uzivatelov
- Zlozky: Application Data, Cookies, Desktop, Favorites, Local Settings, My Documents, Start Menu.....
- su umiestnene v Documents and Settings

Profily vo WIN7

- D&S premenovane na Users, odstranenie prefixu "My"
- zlozka AppData je jednotne ulozisko pre vsetky uzivatelske nastavenia.
    - Local - localne nastavenia, necestuju s pofilom, odpoveda Local Settings/Application Data v XP
    - Roaming - cestuju s profilom, odpoveda Application Data v XP
    - LocalLow - umoznuje zapis low-integrity procesom
- All Users premenovane na Public, Default User premenovane na Default
- slozka Application data premiestnena na %systemdrive%/ProgramData
- Kompatibilita so starymi aplikaciami je zaistena pomocou odkazov na povodne umiestnenie (Junction Points) Everyone:ListContent:Deny
- uzivatelia mozu zdielat subory priamo z uzivatelskeho profilu
- Roaming -moznost synchronizovat nastavenie registrov HKCU (ntuser.dat) automaticky na pozadi behom prihlasenia
- Roaming - Vista+ profil nie je kompatibilny s XP
- praca s profilami - system - system properties - zalozka advanced - user profiles -- mazanie, koprivovanie, zmena typu profilu

UAC

- ked sa admin prihlasi, vygeneruju sa 2 access tokeny - obycajny a privilegovany. Pouziva obycajny a ked potrebuje vykonat cinnost vyzadujucu pouzitie administratorkeho uctu zobrazi sa dialog vyzadujuci potvrdenie privilegovaneho uctu. Toto sa nevztahuje na built-in Administrator ucet, v defaultnom nastaveni.
- Windows spozna ktora applikacia vyzaduje administratorske prava podla
    - Atributu aplikacie - nastavi user
    - Manifestu ktory vytvoril programator
    - Heurisiky (nazov setup.exe install.exe ...) len 32bit aplikacie
- programy v startup zlozke (alebo v kluci run) vyzadujuce provrdenie su automaticky blokovane
- control panel (start napisat UAC) alebo group policy - windows settings/security settings/local policies/security options/user account control

UAC virtualization

- starsie aplikacie mozu vyzadovat zapis do chranenych oblasti (program files, winDir, HKLM/software)
- tieto poziadavky su presmerovane do AppData/Local/VirtualSotre/
- ak aplikacia robi zmenu uz existujuceho suboru, najprv sa tento subor skopiruje do virtual store a az potom ho aplikacia moze editovat
- Aplkikacia bude stale vnutorne pristupovat k povodnemu umiestneniu, tj ked subor utovrim cez aplikaciu uvidim tam aj subory z virtual store, v chranenom umiestneni
- nefunguje ak je aplikacie 64bit, bezi s admin pravami, existuje manifest spustitelneho suboru, administrator nema pristup k chranenemu zdroju (v takomto pripade by aplikacia zlyhala aj na strasom systeme)

Mandatory Integrity Control

- procesy nesmu zapisovat do objektov (subory, kluce registrov) vyssej urovne, ale mozu ich citat
- 3 urovne
    - Low - proces moze zapisovat len do lokalit oznacenych ako low
    - Medium - bezny uzivatel, zapisovat moze do low a medium
    - High - administrator
- ked sa user prihlasi je mu vygenerovany access token ktory obsahuje aj integrity label
- predtym nech su vyhodnotene pristupove opravnenia sa najprv porovna uroven uzivatela a objektu. Ak ma uzivatel vysiu alebo rovnaku je to ok a dalej sa vyhodnocuju NTFS opravnenia. Ak ma nizsiu moze len citat bez ohladu na ntfs opravnenia
- Proces dedi integritnu uroven svojho rodica. Ak ma subor potomka tak potomok dedi tu nizsiu uroven z dvoch - bud zo svojho suboru alebo z rodica

NTFS kompresia

- pri poziadavku na subor ho system automaticky dekomprimuje a komprimuje, proces je transparentny
- vzajomne sa vylucuje so sifrovanim (EFS)
- presuvanie suboru kompresiu zachovava, kopirovanie nie. Subory kopirovane do slozky so zapnutou komprimaciou budu komprimovane. Subory ktore su do takejto zlozky len presunute komprimovane nebudu.

Diskove kvoty

- NTFS filesystem
- definuje sa pre uzivatela a pre zväzok (kvota dat pre kazdeho uzivatela na kazdom zväzku na vsetkych diskoch)
- defaultne to mozu len Administors
- soft - generujuce upozornenie, hard - nedaju sa prekrocit

Encypted File System (EFS)

- NTFS filesystem, vylucuje sa s NTFS kompresiou
- data sifrovane simetrickym klucom ktory je chraneny asymetrickym klucom uzivatela. Kazdy symetricky kluc je odlisny pre kazdy subor (FEK - File Encryption Key)
- mozme zakazat alebo vynutit pouzivanie EFS
- neda sa pouzit na roaming profily
- v domenovom prostredi je PKI a certifikaty spravuje centralne
- reset uzivatelskeho hesla znemozni pristup k certifikatu
- sprava certifikatov - zo startu "manage your certificate" alebo cipher (/r:cesta generuje certifikat pre recovery agenta .cer - public key a .pfx - private key)
- vytvorenie recovery agenta: group policy : Computer Configuration/Windows Settings/ Security Settings/Public Key Policies/Encrypting File System - tu musime nahrat .cer subor
- privatny kluc *.pfx mozme potom zo systemu odstranit, siforovat sa bude uz len verejny. Privatny kluc pouzijeme len na obnovu dat.
- ked chceme aby nieto iny mohol tiez pritupovat k sifrovanemu suboru, musi clovek ktory subor sifruje pridat jeho certifikat. Admin na to nestaci.

Offline files

- zaistenie offline pristupu k datam v zdielanych zlozkach
- su ulozene do cahce na lokalnom disku - %systemroot%/CSC
- nastavenia na strane serveru:
    - default - iba subory ktore user vyberie su dostupne offline
    - ziadne subory nie su dostupne offline
    - vsetky subory ktore user otvori su automaticky dostupne offline
- pri prvnom nacitani sa subor ulozi do chache, zapis ale prebieha do vzdialeneho suboru, ak nie je dostupny nefunguje ani !citanie! ani zapis - vhodne len pomala siet
- platia rovnake opravnenie pre subory offline ako by platili online
- konflikt - uzivatel vyberie zachovat obe alebo jednu z nich.
- Podporuje EFS, sifruje pomocou kluca uzivatela ktory ten subor spritupnil offline

BitLocker

- dotupny pre win7 vo verzii ultimate a enterprise
- sifrovanie vsetkeho vramci celej jednotky vratane jednotky s windows. Po zaonuti su vsetky subory na jednotke automaticky sifrovane (nemozme si vybrat ano/nie)
- BitLocker To Go - nova funcia win7, sifrovanie prenosnych zariadeni (flash, ex. disk)
- nie je zavisly na uzivatelskych uctoch, je on/off pre vsetkych userov a user groupy
- sifrovanie mozu zapnut iba spravci
- vyuziva TMP chip, ktory byva naistalovany na pocitacoch podporujucich pokrocile funkcie zabezpecenia
- pri spusteni pc s TMP a zapnutym BitLockerom kontroluje TMP ci nie je system v stavu ktory moze predstavovat riziko. (Chyba na disku, zmeny v Biose...) Ak ano BitLocker necha odiel zamknuty, dokedy nezadame heslo pre obnovenie.
- heslo TMP chipu sa vytvori pri prvej inicializacii chipu
- Mozme nastavit pomocou BitLocker
    - zakaz pouzivat nesifrovane prenosne disky
    - vynutit pouzivanie smard-card pre spristupnenie obsahu prenosnych diskov
    - zakazat prenosne disky ktore nie su nakonfigurovane BL TO GO
    - vynutit zakaz niektorych recovery metod (ktore som tu neposisoval, viz slid)

Linky

- ShortCut - subor s priponou .lnk
- Symlink - symbolicky odkaz na ciel, system sa k tomu sprava ako k druhemu objektu nie ako ku ShortCut kde sa k nemu sprava ako s suboru
- Hardlink - musi byt na rovnakom volume a diskovym odielu. Je to dalsi zapis to tabulky existence suboru, akakolvek uprava zmeni ciel a subor sa zmaze az ked sa zmazu vsetky harlinky
- JunctionPoint - ukazuje na slozku pomocou absolutnej cesty. Windows automaticky presmeruvava cestu do cielovej zlozky.
- CMD mklink

Ovladace

- driver store - centralne uloziste vsetkych ovladacov (predtym ako su nakopirovane do cieloveho umiestnenia) system32/DriverStore
- driver package - balicek obsahujuci vsetky subori ovladaca (.sys, .inf, .man, .pnf)
- driver stagging, ranking a signing
- ovladace sa neistaluju, su len niekam nakopirovane
- je mozne nastavit aby uzivatelia mohli provest stagging niektorych ovladacov, pomocou tzv. device setup class (vsetky monitory, usb, tlaciarne)

Stagging

- pridanie ovladaca do driver store.
- prebieha ako LocalSystem.
- pridanie driveru vyzaduje admin prava.
- dojde k overeniu, ulozeniu do DS a indexacii pre rychlejsie vyhladanie.
- overenie
    - package musi byt kompletny (inf specifikuje vsetky potrebne subory)
    - behom instalacie nesmu zobrazit ziadne okno ktore vyzaduje interakciu
    - nesmu byt na black-liste zlych ovladacov
    - pre x64 windows musia byt ovladace podpisane doveryhodnym certifikatom
- ked je dokonceny stagging, moze lubovolny user pripojit dane zariadenie a windows automaticky nainstaluje ovladace. To neplati ked je Plug and Play sluzba vypnuta.

Ovladace zariadeni

- je mozne zakazat/povolit instalaciu urcitych zariadeni
- nastroje pnputil.exe verifer.exe sigtool.exe sigverif.exe

Uspora energie

- 3 rezimy - performance, balanced, power saver
- sleep mode: hibernation, sleep, hybrid - kombinacia tych dvoch
- wake timers - moznost prebudit zo sleep mode pre spustenie nejakej ulohy
- programy mozu branit v prechode do sleep mode (prehravanie videa)
- nastroj powercfg (/requests /energy /lastwake)

Sluzby

- dlhodobo beziace aplikacie na pozadi, typicky sa spustaju pri starte
- cela rada systemovych funckii je takto riesena DHCP cleint, Plug and Play
- automatic, automatic - delayed, manual, disabled
- zavislosti na sluzbach (automatic zavisi na manual/disabled)
- bezia pod jednym z uctov Local Systen, Network Service, Local Service, to nie je bezpecne, preto moze sluzba specifikovat ktore opravnenia, prava, pristup na siet vyzaduje (zadava programator)
- preshutdown noticication - umozni sluzbe sa bezpecne vypnut v pripade vypnutia
- trigger start - metoda zapnutia/vypnutia inak ako pri starte systemu
- nastroj sc.exe

Group Policy

- caste hodnoty - enabled, disabled, not configured
- 2 casti politik - computer configuration - nastavenia specificke pre pc, user configuration - specificke pre uzivatelsky ucet
- Local Group Policy -v XP iba jedno nastavenie od Vista+ 3 nastavenia:
    1. Local Policy Object - vsetci uzivatelia (cast computer configuration)
    2. Administrators / Non-Administrators Local GPO - jedna na vsetkych Administrators druha na vsetkach ostatnych
    3. User Specific Loval GPO - aplikovana na konkretneho usera, na skupinu nelze
    - cisla udavaju poradie aplikacie politik, nastavenia sa mozu prepisovat, posledna vyhrava. (pozor na hodnoty non-configured)

Dodatok

- nastroj event viewer - logy, 2 typy - aplikacie a system
- nastroj task scheduler - umoznuje obist UAC -> C:\windows\System32\schtasks.exe /run /tn "TaskName" - dam do shortcut a ak ma uloha high privileges obidem UAC. Do ulohy mozem umiestnit napriklad spustie aplikacie, vyzadujucej admin prava.