UAC - User Account Control (Řízení uživatelských účtů)

UAC, neboli uživatelské řízení účtů, slouží pro rozdělení spuštěných úloh do 2 skupin(úrovní): takové, které si vystačí s běžným uživatelským účtem a takové, které ke svému běhu vyžadují správcovské oprávnění. To umožňuje práci Správce i pod běžným uživatelským účtem, a jen v případě potřeby povýšení úlohy na správcovskou úroveň.

Tedy, jestliže máme aplikaci vyžadující správcovská práva, UAC zobrazí výzvu k dočasnému povýšení dané úlohy do správcovské úrovně. V případě práce pod účtem s administrátorskými právy stačí jen potvrdit tlačítko *Continue* (*Pokračovat*). Na druhou stanu v případě přihlášení uživatele pod standardním účtem je se zobrazí výzva k přihlášení k účtu s administrátorskými právy.

Toto základní chování se nazývá *Admin Approval mode* (*Režim schválení správce*), v tomto režimu aplikace spouštěné jako správcovské vyžadují ke svému běhu specifické povolení.

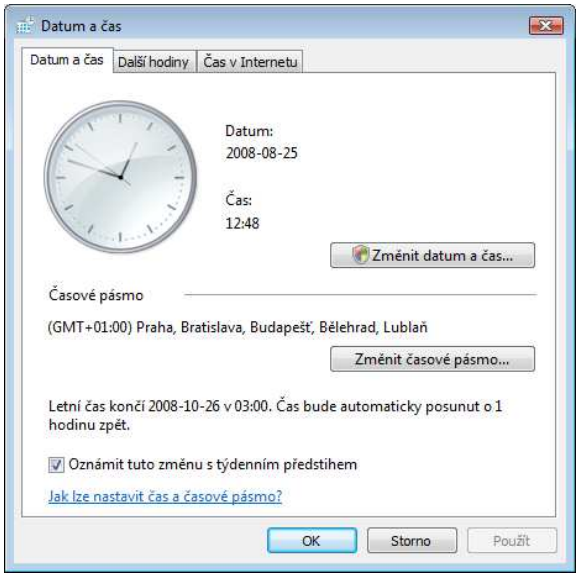
Poznámka: Administrator accounts (Správcovské účty) – Správcovský účet je účet ve skupině *Administrators*. UAC nefunguje v účtu vestavěného Správce, jelikož ve výchozím nastavení je vypnut *Režim schválení správce.*

UAC je podstatným prvkem ochrany před spouštěním nevyžádaných aplikací, jelikož většinu práce je vykonáváno v režimu běžného uživatele a povýšení do správcovského módu vyžaduje potvrzení uživatele.

Poznámka z praxe: Častým jevem pokročilejších uživatelů přecházejících z Windows XP je vypínání UAC, ačkoliv tím degradují jeden z důležitých a přínosných bezpečnostních prvků Windows Vista a Windows 7.

Jak UAC funguje?

Při běžné práci např. v Microsoft Word, nebo při změnách visuálního vzhledu se běžný uživatel nebo správce s UAC příliš nesetká. Změna nastává v případě, kdy chcete vykonat úlohu potřebující ke svému běhu práva správce, např. změna systémových hodin, instalace aplikací apod. Tyto úkony Microsoft označil symbolem čtyřbarevného štítu.



Po kliknutí na symbol štítu je uživatel vyznán k potvrzení spuštění dané úlohy v režimu správce, příp. případně pro přihlášení a získání potřebného oprávnění ke spuštění dané úlohy. Ve Windows 7 je navíc možno ještě nastavit úroveň UAC, čímž dokážeme značně zredukovat počet hlášení UAC.

Další vlastností UAC je zobrazení výzvy v případě spuštění např. instalace aplikace, která není digitálně podepsána nebo ověřena, s dotazem zda danou aplikaci chceme opravdu spustit. V případě běžného uživatele se opět zobrazí žádost o přihlášení pod účtem s právy správce systému.

Naopak aplikace digitálně podepsána zobrazí jen výzvu k povýšení na úroveň správce. V případě použití běžného účtu bude opět vyžadováno přihlášení.

Poznámka: Digitální podpisy se používají pro ověření pravosti vydavatele spustitelné aplikace. Důvěryhodní vydavatelé se kontrolují podle seznamu vydavatelů na daném počítači. Tento seznam obsahuje vydavatele jako Microsoft Corporation nebo externí zprostředkovatele certifikátů Thwait nebo VeriSing.

Secure Desktop

Při zobrazení jakékoliv výzvy UAC dojde k vytvoření snímku obrazovky a jeho zobrazení po dobu zobrazení výzvy což znemožní jakoukoliv jinou práci, nežli dojde k potvrzení výzvy. Stejný systém je též využit pro úvodní nebo přihlašovací okno. Tento způsob byl zvolen za důvodu zvýšení významu zabezpečení a také aby nedocházelo k překrytí výzvy jinými okny, které by si pak uživatel nemusel všimnout.

Zpětná kompatibilita

Ve Windows Vista a Windows 7 byl vytvořen systém zpětné kompatibility pro programy, které byly naprogramovány, aby mohli zapisovat kamkoliv. Jelikož Windows Vista a Windows 7 chrání Registry a Souborový systém, jsou pro tyto případy důležité systémové soubory virtualizovány, což zápisy směřované do chráněné zóny přesměruje do zóny uživatelské. Celý tento proces je automatický a pro uživatele skrytý.

Uživatelské účty

Jak již bylo řečeno podle UAC je uživatel Windows 7 rozdělen do 2 kategorii: Běžný uživatel a správce. Kvůli zvýšení bezpečnosti ve výchozím nastavení všichni uživatelé (kromě vestavěného administrátora) pracují jako běžní uživatelé a jen v případě potřeby dojde k povýšení dané úlohy do správcovského režimu.

Účet správce -Administrator

Správcem se stane každý uživatel, jenž je součástí skupiny Administrators. Člen skupiny Administrators má úplný a neomezený přístup k příslušnému počítači nebo doméně. Avšak jen Vestavěný správce (Build-in Administrator) není ve výchozím nastavení podřízen UAC.

Běžný účet – Standart Account

Běžným účtem se myslí účet náležící do skupiny Users a nemůže provádět nechtěné ani úmyslné změny systému, avšak může spouštět většinu aplikací.

Účet Hosta –Guest

Je členem skupiny Guests a má stejná výchozí přístupová práva jako běžný účet, ale účet Hosta (Guest) má více omezení a je možno na nej aplikovat speciální zabezpečení nebo jej úplně zakázat.

Poznámka: Ve Windows 7 se nacházejí i další skupiny uživatelů např. Power Users, jenž je zachován z důvodu zpětné kompatibility nebo např. Backup Operators, jejíž člen může pro účely zálohování a obnovování dat překonat zabezpečující omezení.

Nastavení zásad zabezpečení

Často bylo zmíněno, jak fungují dané vlastnosti Windows 7 ve výchozím nastavení a nyní se podíváme na podrobnější nastavení a jejich změny v konzoly Editoru místních zásad zabezpečení. Tuto konzoli spustíme přes nabídku start zapsáním **gpedit.msc**. Rozbalíme nabídku Konfigurace počítače (Computer Settings), Nastavení systému Windows (Windows Settings), Nastavení zabezpečení (Security settings), Místní zásady (Local Policies) a Možnosti zabezpečení (Security Options).

Poznámka: Stejné nastavení se nalézá také v konzoly secpol.msc, rozbalíme nabídku Místní zásady (Local Policies) a Možnosti zabezpečení (Security Options)

Zde se nachází následující podrobné nastavení pro UAC:

- **Řízení uživatelských účtů: Chování výzvy ke zvýšení oprávnění pro správce v Režimu schválení správce** – Toto nastavení zásad řídí chování výzvy ke zvýšení oprávnění pro správce. Oproti Windows Vista, byla ve Windows 7 tato možnost značně rozšířena a umožňuje podrobnější nastavení.

  Možnosti:

  - **Zvýšit bez zobrazení výzvy:** Umožňuje privilegovaným účtům provést operaci vyžadující zvýšení oprávnění bez zadání souhlasu nebo pověření.

    Poznámka: Tuto možnost použijte pouze ve velmi omezených prostředích.

  - **Vyzvat k zadání pověření na zabezpečené ploše:** Pokud operace vyžaduje zvýšení oprávnění, zobrazí na zabezpečené ploše výzvu pro uživatele k zadání jména a hesla privilegovaného uživatele. Zadá-li uživatel platná pověření, bude operace pokračovat s nejvyššími oprávněními uživatele.
  - **Vyzvat k zadání souhlasu na zabezpečené ploše:** Pokud operace vyžaduje zvýšení oprávnění, zobrazí na zabezpečené ploše výzvu pro uživatele k výběru možnosti Povolit nebo Zakázat. Vybere-li uživatel možnost Povolit, bude operace pokračovat s nejvyššími možnými oprávněními daného uživatele.
  - **Vyzvat k zadání pověření:** Pokud operace vyžaduje zvýšení oprávnění, zobrazí výzvu pro uživatele k zadání uživatelského jména a hesla pro správu. Zadá-li uživatel platná pověření, bude operace pokračovat s příslušnými oprávněními.
  - **Vyzvat k zadání souhlasu:** Pokud operace vyžaduje zvýšení oprávnění, zobrazí výzvu pro uživatele k výběru možnosti Povolit nebo Zakázat. Vybere-li uživatel možnost Povolit, bude operace pokračovat s nejvyššími možnými oprávněními daného uživatele.
  - **Vyzvat k zadání souhlasu pro binární soubory nepocházející z Windows:** (Výchozí) Pokud operace jiné aplikace než společnosti Microsoft vyžaduje zvýšení oprávnění, zobrazí na zabezpečené ploše výzvu pro uživatele k výběru možnosti Povolit nebo Zakázat. Vybere-li uživatel možnost Povolit, bude operace pokračovat s nejvyššími možnými oprávněními daného uživatele.

  UAC je možno také nastavit přes Ovládací panely\Centrum Akcí\Změnit nastavení nástroje Řízení uživatelských účtů. Zde je možno nastavit 4 úrovně UAC:

  1. **Vždy mne upozornit v těchto případech:**
     a. Pokud se programy pokusí nainstalovat software nebo provést změny v počítači.
     b. Pokud provedu změnu v nastavení Windows.
  2. **Výchozí – Pouze pokud se programy pokusí provést změny v počítači**
     a. Neupozorňovat, pokud změním nastavení systému Windows
  3. **Pouze pokud se programy pokusí provést změny v počítači (nestmívat plochu)**
     a. Neupozorňovat, pokud změním nastavení systému Windows
  4. **Nikdy mne neupozorňovat v těchto případech:**
     a. Pokud se programy pokusí nainstalovat software nebo provést změny v počítači

b. Pokud provedu změny v nastavení systému Windows

- **Řízení uživatelských účtů: Chování výzvy ke zvýšení oprávnění pro standardní uživatele** – Tato zásada nastavuje, zda se má běžnému uživateli zobrazit výzva nebo zda má být automaticky *zamítnuta (!)*.
- **Řízení uživatelských účtů: Povolit aplikacím UIAccess zobrazit výzvu ke zvýšení oprávnění bez použití zabezpečené plochy –** Toto nastavení určuje, zda mohou aplikace UIAccess (User Interface Accessibility neboli UIA) automaticky zakázat u zabezpečené plochy výzvy ke zvýšení oprávnění používané standardním uživatelem
- **Řízení uživatelských účtů: Při zobrazení výzvy ke zvýšení oprávnění přepnout na zabezpečenou plochu –** toto nastavení vypne zabezpečenou plochu
- **Řízení uživatelských účtů: Režim schválení správce pro integrovaný účet správce -** Toto nastavení určuje, zda se budou vestavěnému účtu správce zobrazovat výzvy UAC.
- **Řízení uživatelských účtů: Spustit všechny správce v Režimu schválení správce -** Toto nastavení zabezpečení určuje chování všech zásad UAC pro celý systém.
- **Řízení uživatelských účtů: Virtualizovat chyby zápisu do souboru a registru do umístění jednotlivých uživatelů** - Toto nastavení zabezpečení umožňuje přesměrování zastaralých chyb zápisu aplikací do definovaných umístění v registru i v systému souborů. Tato funkce zabraňuje spuštění aplikací, které byly v minulosti spuštěny v režimu správce a zapsaly data spuštění aplikace do adresářů %ProgramFiles%, %Windir%; %Windir%\system32 nebo HKLM\Software\....
- **Řízení uživatelských účtů: Zjistit instalace aplikací a zobrazit výzvu ke zvýšení oprávnění -** Toto nastavení zabezpečení určuje chování zjišťování instalací aplikací v celém systému, tedy zda se má zobrazit výzva při instalaci aplikací.
- **Řízení uživatelských účtů: Zvýšit oprávnění pouze u aplikací UIAccess, které jsou nainstalovány v zabezpečených umístěních -** Toto nastavení zabezpečení vynutí požadavek, že aplikace vyžadující spuštění s úrovní integrity UIAccess (označením parametru UIAccess=true v manifestu aplikace) musí být v systému souborů uloženy v zabezpečeném umístění.
- **Řízení uživatelských účtů: Zvýšit oprávnění pouze u podepsaných a ověřených spustitelných souborů -** Toto nastavení zabezpečení vynutí kontrolu podpisu PKI(Programová Kontrola Identity) u všech interaktivních aplikací vyžadujících zvýšení oprávnění.

Zásady omezení softwaru

Zásady omezení softwaru řeší nutnost regulovat spouštění neznámého a nedůvěryhodného softwaru. S rostoucím využitím sítí, Internetu a e-mailu pro obchodní účely se uživatelé setkávají s novým softwarem v mnoha různých podobách. Uživatelé se musí neustále rozhodovat, zda mohou neznámý software spustit. Viry a trojské koně se často snaží uživatele záměrně obelstít, aby došlo k jejich spuštění. Pro uživatele je obtížné se správně rozhodnout, který software mohou spustit, aniž by došlo k ohrožení zabezpečení systému.

Pomocí zásad omezení softwaru je možné identifikovat a určit software, který je možné v počítači spustit, a ochránit tak pracovní prostředí před nedůvěryhodným softwarem. Pro objekt zásad skupiny (GPO) je možné definovat výchozí úroveň zabezpečení **Bez omezení** nebo **Nepovoleno**, tak aby bylo spuštění softwaru při výchozím nastavení povoleno nebo zakázáno. Vytvořením pravidel zásad omezení softwaru lze pro určitý software určit výjimky z této výchozí úrovně zabezpečení. Pokud je například výchozí úroveň zabezpečení nastavena na hodnotu **Nepovoleno**, můžete vytvořit pravidla, která povolují spuštění určitého softwaru. Existují tyto typy pravidel:

- **pravidla algoritmu hash**
- **pravidla certifikátu**
- **pravidla cesty (včetně pravidel cesty registru)**
- **pravidla zóny Internetu**

Zásady omezení softwaru jsou tvořeny výchozí úrovní zabezpečení a všemi pravidly platícími pro objekt zásad skupiny. Zásady omezení softwaru se mohou vztahovat na celou doménu, na místní počítače nebo na jednotlivé uživatele. Zásady omezení softwaru umožňují identifikaci softwaru mnoha způsoby. Díky infrastruktuře založené na zásadách lze rozhodnout, zda může být identifikovaný software spuštěn. Pokud jsou používány zásady omezení softwaru, musí uživatelé při spouštění softwarových programů dodržovat pravidla vytvořená správci.

Zásady omezení softwaru umožňují:

- Řídit možnosti spouštění softwaru v systému. Pokud máte například obavy, že by uživatelé mohli přijmout pomocí e-mailu viry, můžete použít nastavení zásad, které nedovolí spuštění určitých typů souborů z adresáře příloh e-mailů používaného e-mailového programu.
- Povolit uživatelům, kteří se střídají při práci na jednom počítači, spouštět pouze určité soubory. Pokud počítače používá více uživatelů, můžete například nastavit takové zásady omezení softwaru, které zajistí, aby uživatelé neměli přístup k jinému softwaru, než který potřebují k práci.
- Určit, kdo může do počítače přidávat důvěryhodné vydavatele.
- Řídit, zda se budou zásady omezení softwaru vztahovat na všechny uživatele nebo jen na některé uživatele počítače.
- Zabránit spuštění jakýchkoli souborů v místním počítači, organizační jednotce, síti nebo doméně. Pokud je například ve vašem systému známý virus, můžete pomocí zásad omezení softwaru zabránit otevření souboru, který daný virus obsahuje.

Pravidlo algoritmu hash

Hodnota hash je série bajtů s pevně definovanou délkou, která jedinečným způsobem identifikuje softwarový program či soubor. Výpočet této hodnoty provádí algoritmus hash. Při vytvoření pravidla algoritmu hash pro softwarový program vypočítá modul Zásady omezení softwaru hodnotu hash daného programu. Pokusí-li se uživatel spustit softwarový program, je algoritmus hash programu porovnán s existujícími pravidly algoritmu hash pro zásady omezení softwaru. Algoritmus hash daného softwarového programu je vždy stejný bez ohledu na umístění programu v počítači. Pokud je však softwarový program jakkoli pozměněn, změní se i jeho algoritmus hash a přestane se shodovat s algoritmem hash v pravidle pro tento algoritmus vztahujícím se k zásadám omezení softwaru.

Chcete-li například zabránit uživatelům ve spuštění určitého souboru, můžete vytvořit pravidlo algoritmu hash a nastavit úroveň zabezpečení na hodnotu **Nepovoleno**. Soubor lze přejmenovat nebo přemístit do jiné složky, a přesto se jeho číslo hash nezmění. Pokud se však samotný soubor jakkoli změní, změní se i jeho algoritmus hash a může dojít k porušení omezení.

Pravidlo certifikátu

Zásady omezení softwaru umožňují identifikovat software také podle jeho podpisového certifikátu. Můžete vytvořit pravidlo certifikátu, které slouží k identifikaci softwaru a k povolení nebo zákazu spuštění softwaru (v závislosti na úrovni zabezpečení). Například můžete použít pravidla certifikátu, která umožňují automatické spuštění softwaru pocházejícího z důvěryhodného zdroje bez zobrazení výzvy k potvrzení této akce uživatelem. Pravidla certifikátu také můžete použít pro spuštění souborů v zakázaných oblastech operačního systému.

Ve výchozím nastavení nejsou pravidla certifikátu povolena.

Pravidlo cesty

Pravidlo cesty identifikuje software podle cesty k souboru. Pokud je například výchozí úroveň zabezpečení počítače nastavena na hodnotu **Nepovoleno**, můžete přesto jednotlivým uživatelům poskytnout neomezený přístup ke konkrétním složkám. Můžete také vytvořit pravidlo cesty tak, že použijete cestu k souboru a nastavíte úroveň zabezpečení tohoto pravidla na hodnotu **Bez omezení**. Jako obecné cesty lze pro tento typ pravidla použít proměnné prostředí **%userprofile%, %windir%**, **%appdata%, %programfiles%** a **%temp%**. Kromě toho můžete vytvářet pravidla cesty registru. U těchto pravidel je jako cesta použit klíč registru příslušného softwaru.

Tato pravidla jsou určena cestami. Pokud se změní umístění softwarového programu, nebude příslušné pravidlo cesty nadále funkční.

Pravidlo zóny Internetu

Pravidla zón mají vliv pouze na balíčky Instalační služby systému Windows. Pravidlo zóny může identifikovat software ze zóny, která je zadána pomocí aplikace Internet Explorer. Jedná se o tyto zóny: Internet, intranet, servery s omezeným přístupem, důvěryhodné servery a tento počítač.

AppLocker

AppLocker je nová funce systému Windows 7, která je dostupná pouze v edicích Enterprise a Ultimate. Politiky jsou koncepčně podobné jako Zásady omezení softwaru, nicméně mají několik výhod jako možnost uplatnění pouze na vybrané uživatele nebo skupiny a taky možnost uplatnění politik na všechny budou verze daného SW produktu. V textu výše jste se dozvěděli, že pravidla algoritmu hash se vážou k dané verzi programu a musejí být znovu obnovena, kdykoli se program aktualizuje. Politiky AppLockeru se nachází v části „*Computer Configuration\Windows Settings\Security Settings\Application Control Policies*“ zásad skupiny u Windows 7 a Windows Server 2008 R2.

AppLocker závisí na službě **Application Identity Service**. Ta po instalaci systému Windows 7 není ve výchozím nastavení spuštěna, je nastavena na ruční spouštění a je tedy potřeba nastavit automatické

spouštění. Jinak by nastavení, která provedete, neměla efekt. Nicméně po dobu testování je doporučeno ponechat ruční spouštění, pokud byste nastavili nesprávné hodnoty, mohli byste si kompletně uzamknout celý operační systém.

Výchozí pravidla

Výchozí pravidla je množina základních povolujících pravidel, která umožňují spouštění základních aplikací Windows. Jsou velmi důležitá, jelikož AppLocker má zabudované výchozí pravidlo blokovat všechny aplikace, které nejsou explicitně povoleny, tzn. po zapnutí AppLockeru nebudete schopni spouštět žádné aplikace, skripty nebo instalátory, pro které neexistuje žádné povolovací pravidlo. Existují různá výchozí pravidla pro různé typy pravidel. Výchozí pravidla jsou všeobecná pro a mohou být administrátory upravena pro jejich prostředí. Například výchozí pravidlo pro exe soubory je pravidlo cesty. Administrátoři by s ohledem na bezpečnost mohli změnit toto chování na přísnější pravidlo, např. Hash.

Blokující pravidla

Pravidla v AppLockeru mohou být buď povolující, nebo odepírající. Explicitní pravidlo Odepřít přepíše jakékoli povolující pravidlo, jakkoli by toto pravidlo bylo definováno. Toto je jiné chování než to u Zásad omezení softwaru, kde se pravidla mohou přepisovat. Výchozí blokující pravidlo zmíněné výše nezakazuje všechny aplikace, pouze ty, které nemají povolující pravidlo. Musíte tedy přidat blokující pravidlo pouze tehdy, pokud již existuje povolující pravidlo pro danou aplikaci. Pokud byste například chtěli povolit všem uživatelům spouštět Alpha.exe kromě skupiny Účetní, vytvořili byste dvě pravidla. Jedno povolující skupině Everyone a druhé blokující pro skupinu Účetní.

Pravidla pro spustitelné programy

Tato pravidla se uplatňují na soubory s koncovkami .exe a .com. Politiky AppLockeru se primárně soustředí na tato pravidla. Výchozím pravidlem je pravidlo cesty. Ve výchozím nastavení je možno spouštět všechny aplikace v adresářích Windows, Program Files, administrátoři mohou spouštět všechny programy. Je důležité použít výchozí pravidla nebo taková pravidla, která jsou podobná, aby mohl operační systém správně fungovat.

Pravidla pro instalátory

Tato pravidla se uplatňují na soubory s koncovkami .msi a .msp, můžete je tedy využít pro povolení nebo zakázání instalování programů. Ve výchozím nastavení je umožněno skupině Everyone spouštět digitálně podepsané balíčky, všechny instalátory v adresáři **%Windir%\Installer**. Administrátoři mohou instalovat cokoli. Dále je povolena instalace programů pomocí GPO. Mějte však na paměti, že přestože skupina Everyone má možnost spouštět instalátory, přesto potřebuje odpovídající úroveň administrativních oprávnění k provedení instalace.

Pravidla pro skripty

Uplatňují se na soubory s koncovkami .ps1, .bat, .cmd, .vbs a .js. Ve výchozím nastavení je možno spouštět všechny skripty v adresářích **Program Files** a **%Windir%**. Dále je umožněno administrátorům spouštět skripty uložené kdekoli.

DLL pravidla

Uplatňují se na soubory s koncovkami .dll a .ocx. Nejsou při povolení AppLockeru aktivní. Jejich využíváním dochází k určitému výkonnostnímu propadu.

Pravidla vydavatele (Publisher Rules)

Tato pravidla fungují na základě podepisování certifikátem, který byl použit vydavatelem souboru. Na rozdíl od pravidla certifikátu u Zásad omezování softwaru zde nemusíte získat certifikát vydavatele, údaje budou načteny z referenční aplikace. Toto pravidlo nemůžete použít na soubory, které nejsou podepsány. Tato pravidla nabízejí velkou flexibilitu do budoucna, jednou povolíte daného vydavatele a i všechny budoucí verze programu budete moci použít. Nicméně můžete upravit pravidlo tak, aby povolovalo pouze určitou verzi produktu nebo vybraný produkt ne všechny produkty vydavatele.

Pravidlo algoritmu hash a cesty

Tato pravidla fungují stejně jako u Zásad omezení softwaru.

Správa disku

Běžné disky a svazky

Běžný disk je fyzický disk, který obsahuje primární oddíly, rozšířené oddíly nebo logické jednotky. Oddíly a logické jednotky na běžných discích se nazývají běžné svazky. Běžné svazky lze vytvářet pouze na běžných discích.

Počet oddílů, které lze na běžných discích vytvořit, závisí na typu oddílu na disku:

- Na discích s hlavním spouštěcím záznamem (MBR) můžete vytvořit maximálně čtyři primární oddíly, nebo tři primární oddíly a jeden rozšířený oddíl. V rámci rozšířeného oddílu lze vytvořit neomezený počet logických jednotek.
- Na discích s tabulkou oddílu GUID (GPT) můžete vytvořit až 128 primárních oddílů. Protože disky typu GPT nejsou omezeny na čtyři oddíly, není třeba vytvářet rozšířené oddíly ani logické jednotky.

K existujícím primárním oddílům a logickým jednotkám lze přidat více místa jejich rozšířením do sousedícího souvislého volného místa na stejném disku. Chcete-li rozšířit běžný svazek, musí být tento svazek formátován pomocí systému souborů NTFS. Logickou jednotku můžete rozšířit v rámci souvislého volného místa v rozšířeném oddílu, jehož je tato jednotka součástí. V případě, že logickou jednotku rozšíříte více, než představuje volné místo v rozšířeném oddílu, zvětší se tento rozšířený oddíl tak, aby mohl logickou jednotku obsáhnout, pokud za ním následuje dostatek souvislého volného místa.

Dynamické disky a svazky

Dynamické disky nabízejí funkce, které u běžných disků nejsou k dispozici, například možnost vytvářet svazky uložené na více discích (rozložené a prokládané svazky) a možnost vytvářet svazky odolné proti chybám (zrcadlené svazky a svazky typu RAID-5). Všechny svazky na dynamických discích se nazývají dynamické svazky. Existuje pět typů dynamických svazků:

- jednoduché (simple)
- rozložené (spanned)
- prokládané (striped)
- zrcadlené (mirrored)
- svazky typu RAID-5

Jednoduché svazky (Simple Volumes)

Ve Windows 7 (a také Windows Vista), jednoduché svazky mohou obsahovat oddíly běžného disku a jednoduché svazky dynamických svazků. Pokud nepotřebujete žádnou další funkcionalitu z jiných typů dynamických disků, Microsoft doporučuje používat běžné diskové oddíly.

Rozložené svazky (Spanned Volumes)

Rozložené svazky používají volné místo na více fyzických discích pro vytvoření svazku. Množství volného místa pro vytvoření nemusí být na všech discích stejné, může být libovolné a může obsahovat více než jeden kus souvislého volného místa z jednoho fyzického disku. Rozložené svazky zvyšují pravděpodobnost výskytu chyby a tudíž i ztráty dat. Porucha kteréhokoli disku, který je součásti tohoto svazku, vede ke ztrátě celého svazku. Tento typ disku nenabízí prakticky žádné výkonnostní zlepšení, slouží hlavně pro vytvoření velkého svazku z více fyzických disků.

Prokládané svazky, RAID-0 (Striped Volumes)

Prokládaný svazek používá volného místa na více než jednom fyzickém disku. Umožňuje systému zápis malých bloků dat (stripes) mezi všemi disky, čímž distribuuje zátěž mezi disky svazku. Data jsou rozdělena do bloků, první je zapsán na první disk, druhý blok na další atd., zápis probíhá souběžně na všech discích. Tento typ svazku vyžaduje minimálně dva fyzické disky.

Data jsou čtena souběžně ze všech disků svazku, čili prokládaný svazek významně urychluje jak rychlosti čtení, tak i zápisu. Množství místa na obou fyzických discích musí být stejné. Pokud by na jednom disku bylo méně místa než na druhém, použije se menší množství. Svazek není odolný vůči poruchám, pokud selže jeden z disků, přijdeme o celý svazek.

Zrcadlené disky RAID-1 (Mirrored Volumes)

Zrcadlené disky poskytují vyšší dostupnost a odolnost vůči poruchám, ale teoreticky neposkytují vyšší výkonnost. K vytvoření svazku je potřeba stejné množství místa na dvou fyzických discích. Všechny změny, které jsou prováděny na jednom disku, jsou zrcadleny (promítány) také na druhý disk. Pokud selže první disk, zrcadlení je porušeno a druhý z disků je používán, dokud nedojde k opravě nebo výměně prvního disku. Zrcadlení může být následně znovu vytvořeno a informace z jednoho disku se duplikují na druhý. Nevýhodou je potřeba mít například dva 200 GB disky, abyste mohli mít zrcadlený oddíl o velikosti 200 GB.

Svazky typu RAID-5

Tento typ svazků nabízí výší dostupnost, odolnost vůči poruchám a současně vyšší výkonnost. Vyžaduje alespoň tři fyzické disky nebo stejně velké množství volného místa na všech třech discích. Funguje podobně jako prokládaný typ svazku, ale část kapacity slouží k uložení informace o paritě daného bloku dat. Čili pokud jeden disk selže, data jsou obsažena na zbylých discích, nicméně dojdu k propadu výkonnosti, jelikož se musí data vypočítávat z partity a části fyzických dat, kdykoli se s daty pracuje. Vadný disk může být nahrazen a obsah obnoven. Rychlost čtení ze svazku je rychlejší, jelikož jsou data čtena ze všech disků současně. Rychlost zápisu není tak výrazná kvůli potřebě vytvářet paritu. Paritní informace nejsou ukládány pokaždé na stejném disku, ale jsou distribuovány mezi všemi disky. Parita zabere stejné místo, jaké poskytuje jeden disk, čili pokud budete mít tři disky po 200 GB, budete mít 400 GB svazek k dispozici (n-1).

LAB1 – User Account Control

V prvních dvou cvičeních si pohrajeme s pokročilejšími nastaveními ovlivňující chování UAC.

Prerekvizity: win7-base a uživatelské účty Student (Administrators) a Bart (Users).

1) Přihlaste se k **win7-base** pod účtem **Bart**.
2) Zkuste spustit Správu systému (Computer -> Manage).
3) Použijte účet Student a jeho heslo.
4) Odhlaste se od účtu Bart a přihlaste se jako Student.
5) Otevřete Editor místních zásad skupiny (Local Group Policy Editor) např. příkazem **gpedit.msc**
6) Vyberte Konfigurace počítače -> Nastavení systému Windows -> Nastavení zabezpečení -> Lokální nastavení -> Nastavení zabezpečení (Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options).
7) Zakažte položku „**User Account Control: Switch to secure desktop hen promting for elevation**“.
8) Přihlaste zpět jako **Bart** a zkuste spustit Správu systému.
9) V nabídce Start napište **gpedit.msc**, klikněte pravým tlačítkem myši a zvolte Spustit jako administrátor (Run as Administrator). Vraťte zpět předchozí nastavení.
10) Změňte hodnotu „**User Account Control: Behavior of the elevation prompt for standard users na „Automatically deny elevation requests**“.
11) Stále pod účtem Bart zkuste otevřít Správu systému.

LAB2 – UAC ve Windows ala Linux

1) Přihlaste se k **win7-base** pod účtem **Student**.
2) Otevřete Editor místních zásad skupiny pro editaci UAC nastavení.
3) Vyzkoušejte měnit hodnoty v položce „**User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**“ a pro každou změnu spusťte Správu systému. (Pokud bychom chtěli nasimulovat UAC podobně jako v Linuxu bylo by třeba nastavit hodnotu na „**Elevate without prompting**“.)
4) Zakažte položku „**User Account Control: Switch to the secure desktop when prompting for elevation**“ a vyzkoušejte opět spustit Správu systému.
5) Zkontrolujte hodnotu „**User Account Control: Behavior of the elevation prompt for standard users**“, jestli obsahuje „**Prompt for credentials**“.
6) Přihlaste se pod uživatelem **Bart** a zkuste spustit Správu systému.

LAB3 – Omezování aplikací se Software Restriction Policies

V tomto cvičení si vytvoříte pravidlo pomocí SRP pro blokování aplikace Notepad.exe pomocí Hash pravidla.

1) Přihlaste se na **win7-base** pod účtem **Student**.
2) Z nabídky Start spusťte **Poznámkový blok** (Notepad) a poté jej zavřete.
3) Otevřete Editor místních zásad skupiny (Local Group Policy Editor) např. příkazem **gpedit.msc**
4) Vyberte Konfigurace počítače -> Nastavení systému Windows -> Nastavení zabezpečení -> Zásady omezení softwaru (Computer Configuration -> Windows Settings -> Security Settings -

> Software Restriction Policies), klikněte pravým tlačítkem myši a zvolte Nové zásady omezení softwaru.

5) Klikněte pravým tlačítkem myši na Další pravidla (Additional Rules) a zvolte Nové pravidlo algoritmu hash… (New Hash Rule…).
6) Klikněte na tlačítko Procházet… (Browse…) a vyberte z adresáře „**C:\Windows**“ aplikaci **Notepad.exe**. Ujistěte se, že je zvoleno nastavení Nepovoleno (Disallowed) -> OK.
7) Zavřete Editor místních zásad skupiny, restartujte PC. Poté se opět přihlaste a pokuste se spustit Poznámkový blok.
8) Smažte nastavení, která jsme vytvořili v předchozích krocích, opět restartujte a po přihlášení by mělo spuštění opět fungovat.

LAB4 – Omezování aplikací s AppLocker

Nyní si ukážeme omezení stejného typu pouze s využitím politik aplikace AppLocker.

1) Přihlaste se na **win7-base** pod účtem **Student**.
2) Otevřete MMC konzolu Služby (Services) např. příkazem **services.msc**.
3) Vyhledejte službu **Application Identity**. Otevřete její vlastnosti a zvolte typ spouštění na **Automaticky**.
4) Otevřete Editor místních zásad skupiny (Local Group Policy Editor) např. příkazem **gpedit.msc**
5) Vyberte Konfigurace počítače -> Nastavení systému Windows -> Nastavení zabezpečení -> Zásady omezení softwaru -> AppLocker (Computer Configuration -> Windows Settings -> Security Settings -> Application Control Policies -> AppLocker).
6) Klikněte pravým tlačítkem myši na Pravidla spouštění (Executable Rules) a vyberte Vytvořit nové pravidlo (Create New Rule). V průvodci si přečtěte úvodní informace a pokračujte.
7) Na stránce „Oprávnění“ vyberte Odepřít -> Next.
8) Na stránce „Podmínky“ vyberte Vydavatel -> Next.
9) Na stránce „Vydavetel“ klikněte na tlačítko Procházet (Browse) a vyberte z adresáře „**C:\Windows**“ aplikaci **Notepad.exe**. Dále vyberte Zvolit vlastní hodnoty a zvolte následující nastavení -> Vytvořit:
   Při dotazu na Vytvoření nových pravidel zvolte Ano.
10) Zavřete Editor místních zásad skupiny, restartujte PC. Poté se opět přihlaste a pokuste se spustit Poznámkový blok.

LAB5 – Dynamické disky

V následujících cvičeních si ukážeme práci s diskovými oddíly, dynamickými disky a softwarové verzi technologií RAID-0, RAID-1 a RAID-5.

Prerekvizity: **win2008r2-base** s třemi přídavnými disky (VHD soubory), celkově čtyřmi.

1) Přihlaste se na **win2008r2-base** pod účtem lokálního administrátora.
2) Otevřete konzolu Správa disků (Disk Management) např. příkazem **diskmgmt.msc**.
3) V úvodní nabídce Inicializace disků (Initialize Disk) zvolte inicializaci všech disků jako **MBR**.
4) Konvertujte disky 1 a 2 na dynamické. Klikněte pravým tlačítkem myši na příslušný disk a zvolte nabídku Převést na dynamický disk… (Convert to Dynamic Disk…).
5) Spusťte příkazový řádek **cmd**. Konvertujte třetí disk na dynamický pomocí nástroje **Diskpart**:

- **diskpart**
- **list disk**
- **select disk 3**
- **clean**
- **convert dynamic**
- **exit**

6) Vraťte se zpět do konzole Disk Management. Klikněte pravým tlačítkem myši na volné místo disku 1 a vyberte Nový jednoduchý svazek… (New Simple Volume…). Pomocí průvodce vytvořte oddíl:
   - velikost: 20 GB
   - jednotka: D
   - systém souborů: NTFS
   - rychlé formátování
7) Vraťte se do příkazového řádku. Vytvoříme podobný svazek s využitím diskpartu:
   - **diskpart**
   - **select disk 2**
   - **create volume simple size=20480**
   - **list volume**
   - **select volume** *<číslo_oddílu>*
   - **format FS=NTFS Quick**
   - **assign letter=E**
   - **exit**

LAB6 – Spanned Volume

V tomto cvičení si vytvoříme oddíl, který bude tvořen třemi oddíly, každý z různého fyzického disku, ale navenek se bude tvářit jako jeden oddíl o celkové velikosti dané součtem všech tří oddílů. Poté nasimulujeme poruchu jednoho z disků a přesvědčíme se, že tak přijdeme o celý oddíl.

1) Přihlaste se na **win2008r2-base** pod účtem lokálního administrátora.
2) Otevřete konzolu Disk Management např. příkazem **diskmgmt.msc**.
3) Klikněte pravým tlačítkem na **Disk1** a vyberte Nový rozložený svazek… (New Spanned Volume…).
4) V průvodci na stránce Vyberte jednotky (Select Disks) přidejte všechny tři disky a u každého disku zvolte jinou velikost, kterou přispěje daný disk k novému svazku např. 10, 20, 30 GB. Pokračujte dále a připojte nový svazek pod dalším dostupným písmenem.
5) Klikněte pravým tlačítkem myši na **Disk3** a vyberte Offline. Všimněte si, že přijdeme o celý svazek.
6) Uveďte Disk3 do stavu Online.

LAB7 – Stripped Volume

Nyní vytvoříme oddíl, který bude představovat softwarový RAID0, čili polovina data se zapisuje na jeden oddíl a druhá půlka na další. Velikost oddílů musí být shodná a výsledná velikost nového oddílu je rovna součtu velikostí obou oddílů. Výhodou tohoto oddílu je teoreticky dvojnásobná rychlost, ale je zde vyšší nebezpečí selhání dat. Opět nasimulujeme pád jednoho z disků.

1) Přihlaste se na **win2008r2-base** pod účtem lokálního administrátora.
2) Otevřete konzolu Disk Management např. příkazem **diskmgmt.msc**.
3) Klikněte pravým tlačítkem na Disk1 a vyberte Nový prokládaný svazek… (New Stripped Volume…).
4) V průvodci na stránce Vyberte jednotky (Select Disks) přidejte **Disk1** a **Disk2** a nastavte velikost odebraného místa z každého disku na 20 GB. Dokončete průvodce.
5) Opět nasimulujte výpadek disku 2, dojde tak ke ztrátě dat na obou discích.
6) Uveďte Disk2 do stavu Online.
7) Spusťte příkazový řádek. Vytvoříme podobný svazek s využitím diskpartu:
   - **diskpart**
   - **create volume stripe size=10240 Disk=2,3**
   - **list volume**
   - **select volume** *<číslo_oddílu>*
   - **format FS=NTFS Quick**
   - **assign letter=***<písmeno_jednotky>*
   - **exit**

LAB8 – Mirrored Volume

V následujícím cvičení vytvoříme zrcadlený diskový oddíl. Data se budou zrcadlit na druhý disk. Výhodu je tak redundance dat, kdy při výpadku máme kompletní data i na nepoškozeném disku a teoreticky rychlejší čtení z disku. Nevýhodou je pak poloviční velikost oddílu.

1) Přihlaste se na **win2008r2-base** pod účtem lokálního administrátora.
2) Otevřete konzolu Disk Management např. příkazem **diskmgmt.msc**.
3) Klikněte pravým tlačítkem na **Disk1** a vyberte Nový zrcadlený svazek… (New Mirrored Volume…).
4) V průvodci na stránce Vyberte jednotky (Select Disks) přidejte **Disk1** a **Disk2** a nastavte velikost odebraného místa z každého disku na 20 GB. Dokončete průvodce.
5) Zkopírujte na nový svazek libovolná data.
6) Opět nasimulujte výpadek, tentokrát disku 1.
7) Zkopírujte další data na svazku.
8) Uveďte Disk1 do stavu Online. Všimněte si, že svazek hlásí chybu redundance (synchronizace). Klikněte na daný oddíl pravým tlačítkem myši a zvolte Aktivovat svazek (Reactivate Volume).
9) Spusťte příkazový řádek. Vytvoříme podobný disk s využitím diskpartu:
   - **diskpart**
   - **create volume mirror size=10240 Disk=2,3**
   - **list volume**
   - **select volume** *<číslo_oddílu>*
   - **format FS=NTFS Quick**
   - **assign letter=***<písmeno_jednotky>*
   - **exit**

LAB9 – RAID-5

Vytvoříme si oddíl představující softwarové řešení RAID-5. K tomu je potřeba tří oddílů každý na jiném disku stejné velikost. Tentokrát však nepřipojíme nový oddíl pod dalším písmenem, ale do prázdného adresáře. Čili všechna data zapsaná do nového adresáře se budou fyzicky zapisovat do diskového pole. Dále upravíme velikost systémového disku a uvolníme si 25 GB místa. Budeme simulovat výpadek třetího disku a jako náhradní disk využijeme Disk0 a obnovíme tak plnou funkčnost pole.

1) Přihlaste se na **win2008r2-base** pod účtem lokálního administrátora.
2) Otevřete konzolu Disk Management např. příkazem **diskmgmt.msc**.
3) Klikněte pravým tlačítkem na **Disk1** a vyberte Nový svazek typu RAID-5… (New RAID-5 Volume…).
4) Vytvořte si na disku **C** adresář **C:\RAID5**.
5) V průvodci zvolte velikost 20 GB -> Next. Na další stránce nepřidávejte oddílu další písmeno jednotky, ale Připojit do této prázdné složky NTFS: (Mount in the following empty NTFS folder:) a kliknutím na tlačítko Procházet… (Browse…) vyberte adresář **C:\RAID5**. Dokončete průvodce.
6) Klikněte pravým tlačítkem myši na oddíl **C** a zvolte Zmenšit svazek… (Shrink Volume…). Uvolněte si 25 GB místa.
7) Konvertujte Disk0 na dynamický disk.
8) Nasimulujte výpadek třetího disku. Oddíl bude stále dostupný. Klikněte na něj pravým tlačítkem myši a zvolte Opravit svazek… (Repair Volume…) a následně zvolte Disk0.
9) Uveďte Disk3 do stavu Online.