Řízení uživatelských účtů (UAC, User Account Control) [Povinné]

UAC, neboli řízení uživatelských 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 oprávnění správce. 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 **Pokračovat** (*Continue*). Na druhou stanu v případě přihlášení uživatele pod standardním účtem je se zobrazí výzva k přihlášení k účtu s administrátorskými právy.

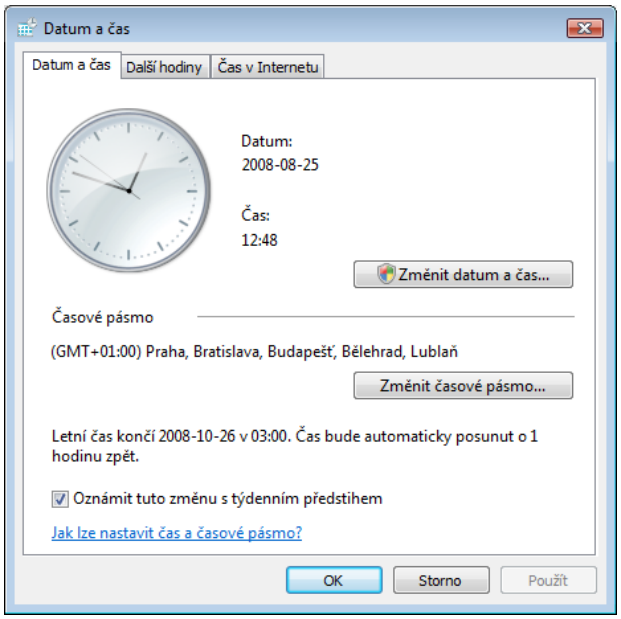
Toto základní chování se nazývá **Režim schválení správce** (*Admin Approval Mode*), v tomto režimu aplikace spouštěné jako správcovské vyžadují ke svému běhu specifické povolení.

> *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.

> *Častým jevem pokročilejších uživatelů přecházejících z Windows XP je vypínání UAC, ačkoliv tím degradují jeden z důležitých a přínosných bezpečnostních prvků systému Windows.*

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 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. Od 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.

> *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 Thawte nebo VeriSign.*

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 byl vytvořen systém zpětné kompatibility pro programy, které byly naprogramovány, aby mohli zapisovat kamkoliv. Jelikož systémy Windows od Windows Vista 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 [Povinné]

Jak již bylo řečeno podle UAC je uživatel Windows 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 něj aplikovat speciální zabezpečení nebo jej úplně zakázat.

> *Ve Windows 10 se nacházejí i další skupiny uživatelů např. Power Users, jenž je zachována z důvodu zpětné kompatibility nebo např. Backup Operators, jejíž člen může pro účely zálohování a obnovování dat překonat zabezpečující omezení.*

Nastavení zásad zabezpečení [Povinné]

Často bylo zmíněno, jak fungují dané vlastnosti Windows 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*) -> Možnosti zabezpečení (*Security Options*).

> *Stejné nastavení se nalézá také v konzoli 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 od 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[1].
- **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. **Pouze pokud se programy pokusí provést změny v počítači** (výchozí)
   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.

[1] Tuto možnost použijte pouze ve velmi omezených prostředích.

- **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 (*Public Key Infrastructure*) u všech interaktivních aplikací vyžadujících zvýšení oprávnění.

Zásady omezení softwaru [Povinné]

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

[Povinné]

AppLocker je funkce systému představená ve Windows 7, která je dostupná pouze v edicích **Enterprise** a **Education** (dříve i Ultimate). Zásady jsou koncepčně podobné **Zásadám omezení softwaru**, nicméně mají několik výhod jako možnost uplatnění pouze na vybrané uživatele nebo skupiny a taky možnost uplatnění zásad na všechny budoucí 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. Zásady **AppLockeru** se nachází v části **Computer Configuration \ Windows Settings \ Security Settings \ Application Control Policies** zásad skupiny.

AppLocker závisí na službě **Application Identity Service**. Ta po instalaci systému Windows 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**.

Společné úkoly

- Pro přístup na server **file** (a jiné) přes síťové rozhraní *Default switch* je nutné použít jeho plně kvalifikované doménové jméno **file.nepal.local**
- Přístupové údaje na server file: **nepal\hstudent** heslo: **aaa**

Lab L00 – konfigurace virtuálních stanic

[Provést]

Připojte sítové adaptéry stanic k následujícím virtuálním přepínačům:

Adaptér (MAC suffix)	LAN1 (-01)	LAN2 (-02)	LAN3 (-03)	LAN4 (-04)
w10-base	Default switch	Nepřipojeno	Nepřipojeno	Nepřipojeno
w10-domain	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno
w2016-dc	Default switch	Private1	Nepřipojeno	Nepřipojeno

Lab LS01 – User Account Control

[Provést]

Cíl cvičení

Vyzkoušet si pokročilejší nastavení ovlivňující chování UAC.

Potřebné virtuální stroje

w10-base

Další prerekvizity

Uživatelský účet **Student**, jenž je členem skupiny **Administrators**.
Uživatelský účet **Bart**, jenž je členem skupiny **Users**.

1. Přihlaste se k **w10-base** pod účtem **Bart**.
2. Zkuste spustit Správu disků (Disk Management) - příkazem diskmgmt.msc, nebo z kontextové nabídky nad tlačítkem Start (Win + X)).
   - Správa disků oznámí, že uživatel nemá odpovídající práva.
3. Uzavřete okno Správy disků
4. Zkuste spustit Správu disků (Disk Management), tentokrát však jako jiný uživatel - V nabídce Start napište **diskmgmt.msc**, klikněte pravým tlačítkem myši a zvolte Spustit jako správce (Run as Administrator)
   - Použijte účet **Student** a heslo **aaa.**
   - Správa disků se otevře s vhodnými právy a tedy bez varování.
5. Odhlaste se od účtu **Bart** a přihlaste se jako **Student**.
6. Otevřete Editor místních zásad skupiny (Local Group Policy Editor) např. příkazem **gpedit.msc**
7. Vyberte Konfigurace počítače -> Nastavení systému Windows -> Nastavení zabezpečení -> Lokální nastavení -> Nastavení zabezpečení (Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options).
8. Zakažte položku User Account Control: Switch to secure desktop when prompting for elevation.
9. Přihlaste zpět jako **Bart** a zkuste spustit Správu disků.
10. V nabídce Start napište **gpedit.msc**, klikněte pravým tlačítkem myši a zvolte Spustit jako správce (Run as Administrator). Vraťte zpět předchozí nastavení.
11. Změňte hodnotu User Account Control: Behavior of the elevation prompt for standard users na **Automatically deny elevation requests**.
12. Stále pod účtem **Bart** zkuste otevřít Správu disků.

Lab LS02 – UAC ve Windows ala Linux [Provést]

Cíl cvičení

Nastavit UAC tak, aby se s uživatelskými účty pracovalo jako v Linuxu, tzn. aby správci počítače běželi vždy pod oprávněními správce a standardní uživatele museli zadat pověření.

Potřebné virtuální stroje

w10-base

Další prerekvizity

Uživatelský účet **Student**, jenž je členem skupiny **Administrators**.
Uživatelský účet **Bart**, jenž je členem skupiny **Users**.

1. Přihlaste se k **w10-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 disků (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 disků.
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 disků.

Lab LS03 – Omezování aplikací pomocí Zásad omezení softwaru [Provést]

Cíl cvičení

Zamezit spouštění konkrétní aplikace vytvořením hash pravidla zásad omezení softwaru.

Potřebné virtuální stroje

w10-base

1. Přihlaste se na **w10-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 (New Software Restriction Policies).
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 a spusťte příkaz **gpupdate /force**. Odhlaste se a znova přihlaste a pokuste se spustit **Poznámkový blok**.
8. Smažte nastavení, která jsme vytvořili v předchozích krocích, spusťte příkaz **gpupdate /force** a opět se odhlaste. Po přihlášení by mělo spuštění opět fungovat.

Lab LS04 – Omezování aplikací pomocí nástroje AppLocker

[Provést]

Cíl cvičení

Zamezit spouštění konkrétní aplikace vytvořením pravidla vydavatele nástroje AppLocker.

Poznámka:

Potřebné virtuální stroje

w10-domain
w2016-dc

1. Přihlaste se na **w2016-dc** pod účtem **testing\administrator**.
2. Otevřete Správu zásad skupin (Group Policy Management)
   - Start → Windows Administrative Tools → **Group Policy Management** nebo příkazem **gpmc.msc**
   - Jedná se obdobu nástroje Editor místních zásad skupiny (Local Group Policy Editor, gpedit.msc) pro centrální konfiguraci počítačů v doméně.
3. Vytvořte objekt zásady skupiny (GPO) **Applocker policy**
   - Klikněte pravým na doménu **testing.local** a zvolte Create a GPO in this domain, and Link it here…
   - Jako název (Name) zvolte **Applocker policy** a u Source Starter GPO ponechte (**none**)
   - Potvrďte OK
4. Z kontextové nabídky (pravý klik) objektu **Applocker policy** zvolte Upravit (Edit). Objeví se okno Editor správy zásad skupiny (Group Policy Management Editor)
5. Vyberte Konfigurace počítače -> Zásady -> Nastavení systému Windows -> Nastavení zabezpečení -> Zásady omezení softwaru -> AppLocker (Computer Configuration -> Policies -> 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 (Permissions) vyberte **Odepřít** (Deny) a pokračujte pomocí Další (Next).
8. Na stránce Podmínky (Conditions) vyberte **Vydavatel** (Publisher) a pokračujte pomocí Další (Next).
9. Na stránce Vydavatel klikněte na tlačítko Procházet (Browse) a vyberte z adresáře **C:\Windows** aplikaci **Notepad.exe**.
   - Nyní můžete zvolit, které z údajů ze zvolené aplikace se použijí jako pravidlo
     i. Při zaškrtnutí Zvolit vlastní hodnoty (Use custom values) lze jednotlivé hodnoty editovat - všimněte si změn u verze souboru (File version)
10. Nastavte posuvník definice pravidla na úroveň Název souboru (File name) a pokračujte pomocí Další (Next).
11. Na stránce Výjimky (Exceptions) můžete obdobným způsobem nadefinovat výjimky z nastavovaného pravidla. Pokračujte pomocí Další (Next).
12. Na stránce Name (Název) pojmenujte pravidlo (můžete ponechat výchozí název) a pokračujte Vytvořit (Create)
    - Při dotazu na Vytvoření výchozích pravidel zvolte **Ano** (Yes).
13. Zvolte uzel **Applocker** a z kontextové nabídky (pravý klik) zvolte Vlastnosti (Properties). Vyberte kartu Vynucení (Enforcement)
14. U pravidel vydavatele (Executable rules) zaškrtněte Nakonfigurováno (Configured). Z nabídky vyberte Pouze audit (Audit only). Potvrďte tlačítkem Použít (Apply)

15. Nyní nastavím spouštění služby Identita aplikací (Application identity)
16. V Editoru správy zásad skupiny objektu **Applocker policy** (Group Policy Management Editor) vyberte Konfigurace počítače -> Zásady -> Nastavení systému Windows -> Nastavení zabezpečení -> Systémové služby (Computer Configuration -> Policies -> Windows Settings -> Security Settings -> System Services).
17. Mezi službami najděte službu Identita aplikace (Application Identity), z kontextové nabídky vyberte Vlastnosti (Properties), zaškrtněte Nastavit tuto zásadu (Define this policy settings) a vyberte Automaticky (Automatic). Potvrďte tlačítkem OK.
18. Zavřete Editor správy zásad skupiny (Group Policy Management Editor)

19. Přihlaste se na **w10-domain** pod účtem **testing\Bart**.
20. Pokuste se spustit **Poznámkový blok** (notepad.exe).
21. Spusťte příkaz **gpupdate /force**.
22. Otevřete MMC konzolu Služby (Services) např. příkazem **services.msc**.
23. Vyhledejte službu Identita aplikace (Application Identity) a zkontrolujte její stav
24. Pokuste se spustit **Poznámkový blok** (notepad.exe).
    - Povede se, protože jsme nastavili pouze audit.
25. Otevřete Prohlížeč událostí (Event Viewer) např. příkazem **eventvwr.msc**.
26. Přejděte do Protokoly aplikací a služeb -> Microsoft -> Windows -> Applocker (Applications and Services Log -> Microsoft -> Windows -> Applocker) a prozkoumejte log **Exe and DLL**
    - Naleznete zde Varování (Warning) o spuštění aplikace notepad.exe.
27. Přihlaste se na **w2016-dc** pod účtem **testing\administrator**.
28. Upravte zásadu **Applocker policy** a přepněte **Applocker** do režimu vynucení pravidel (Enforce rules)
    - Zopakujte body 2, 4, 5, 13, 14, 18
29. Přihlaste se na **w10-domain** pod účtem **testing\Bart**.
30. Pokuste se spustit **Poznámkový blok** (notepad.exe).
    - Nepovede se, protože jsme nastavili vynucení.
31. Zkontrolujte protokol událostí
    - Zopakujte body 25, 26