

Desktop systémy Microsoft Windows

IW1/XMW1 2012/2013

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 19.11.2012

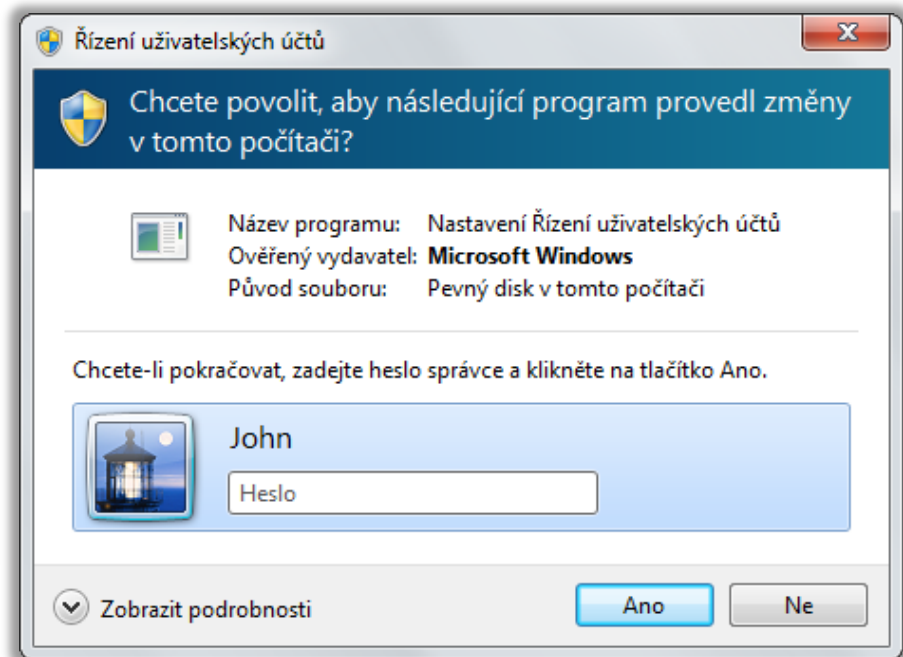
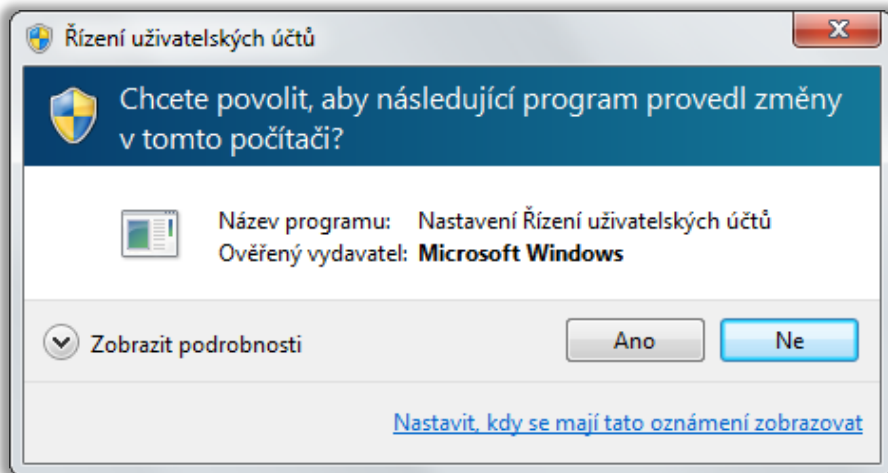
Řízení uživatelských účtů (UAC)

Řízení uživatelských účtů (UAC)

- **User Account Control**
- Umožňuje zvyšování (elevaci) oprávnění
- Zvyšuje bezpečnost systému
 - Explicitní souhlas / zadání pověření (*credentials*)
- Úkony, které vyžadují zvýšení oprávnění graficky odlišeny ikonou štítu
- Dvě úrovně nastavení
 - Základní nastavení v ovládacích panelech
 - Pokročilé nastavení v zásadách skupiny



Výzvy k zadání souhlasu a pověření

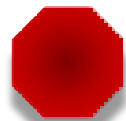


Zvyšování (elevace) oprávnění

- Proces zpřístupnění oprávnění správce uživateli
- Všichni přihlášení uživatelé (včetně správců) běží s oprávněními standardního uživatele
- Vždy pouze pro konkrétní úkon (např. spuštění programu, změnu nastavení systému, ...)
 - Oprávnění pro ostatní úkony musí být zvýšeny zvlášť
- Režim schválení správce (*Admin Approval mode*)
 - Správce musí explicitně potvrdit zvýšení oprávnění
 - Potvrzení formou souhlasu nebo zadání pověření

Standardní uživatel

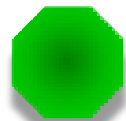
Přístupový token s oprávněními
správce (jiný uživatel)



Správa počítače
(**compmgmt.msc**)



Zvýšení oprávnění
(Zadání pověření)

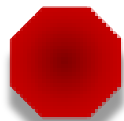


Plocha
(**explorer.exe**)

Přístupový token s oprávněními
standardního uživatele

Správce v režimu schválení správce

Přístupový token s oprávněními
správce



Správa počítače
(**compmgmt.msc**)

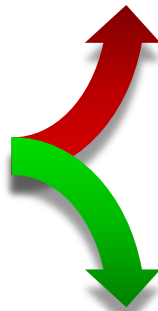


Zvýšení oprávnění

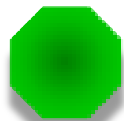
(Zadání pověření či potvrzení)



Přihlášení



Spuštění



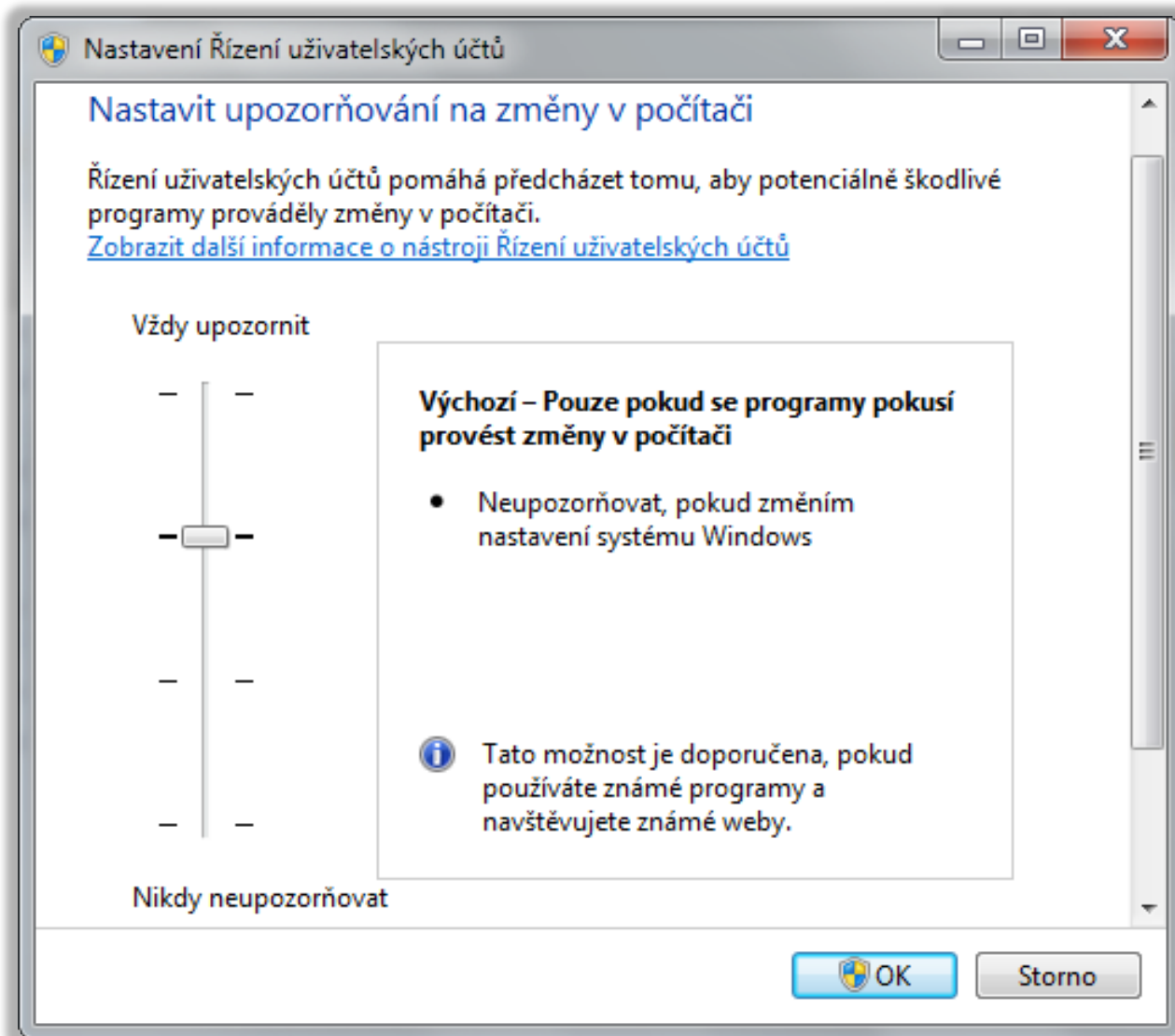
Plocha
(**explorer.exe**)

Přístupový token s oprávněními
standardního uživatele

Zabezpečená plocha (Secure Desktop)

- Zabraňuje modifikaci plochy (obrazovky) v době, kdy je zobrazena výzva k zvýšení oprávnění
 - Plocha je v této době nepřístupná (zobrazen snímek)
- Uživatel musí do 150 sekund reagovat na výzvu
 - Po 150 sekundách je zvýšení oprávnění automaticky zamítnuto a zabezpečená plocha zrušena

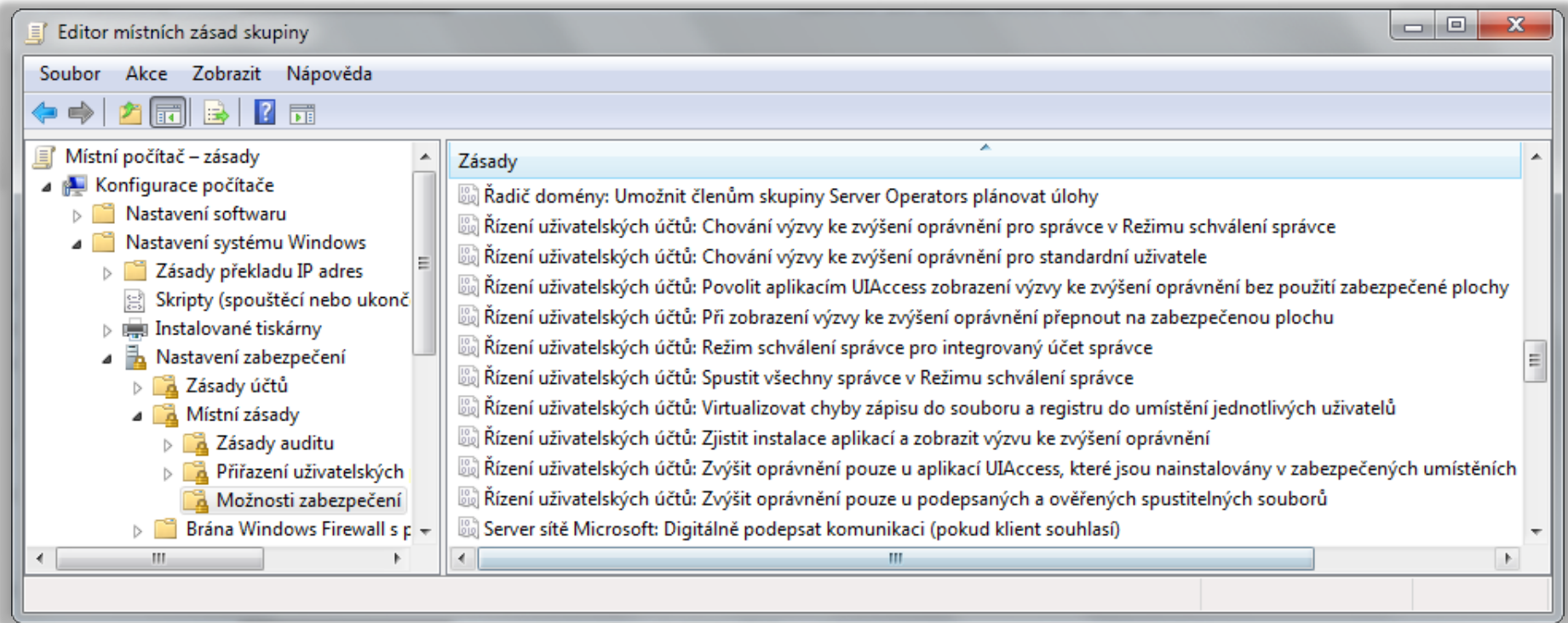
Základní nastavení



Možnosti základního nastavení

- Vždy upozorňovat
- Upozorňovat pouze pokud se programy pokusí provést změny v počítači
 - Povolit provádění změn v systému Windows nástroji pocházejícími ze systému Windows (jsou podepsány)
- Upozorňovat pouze pokud se programy pokusí provést změny v počítači (nestmívat plochu)
- Nikdy neupozorňovat
 - Povolovat pro správce resp. zamítat pro standardního uživatele všechny žádosti o zvýšení oprávnění

Pokročilé nastavení



Zásady ovlivňující chování UAC (1)

- Chování výzvy ke zvýšení oprávnění pro správce v Režimu schválení správce
 - Zvýšit bez zobrazení výzvy
 - Vyzvat k zadání souhlasu (na zabezpečené ploše)
 - Vyzvat k zadání pověření (na zabezpečené ploše)
 - Vyzvat k souhlasu pro binární soubory neurčené pro systém Windows
 - Požadovat souhlas pouze v případě, že zvýšení oprávnění vyžaduje aplikace, jenž není součástí systému Windows
 - Výchozí nastavení

Zásady ovlivňující chování UAC (2)

- Chování výzvy ke zvýšení oprávnění pro standardní uživatele
 - Automaticky zamítnout požadavky na zvýšení
 - Vyzvat k zadání pověření (na zabezpečené ploše)
 - Výchozí nastavení různé (u serverů většinou zadat pověření, u edicí Enterprise zamítnout, u Professional zadat pověření)
- Povolit aplikacím UIAccess zobrazení výzvy ke zvýšení oprávnění bez použití zabezpečené plochy
 - Povolením mohou uživatelé UIAccess aplikací (např. vzdálené pomoci) reagovat na výzvy ke zvýšení oprávnění
 - Ve výchozím nastavení zakázáno

Zásady ovlivňující chování UAC (3)

- Při zobrazení výzvy ke zvýšení oprávnění přepnout na zabezpečenou plochu
 - Při povolení vynucuje použití zabezpečené plochy při výzvách k zadání souhlasu / pověření
 - Při zakázání lze požádání vynutit použití zabezpečené plochy v nastavení chování výzev pro správce / standardní uživatele
 - Ve výchozím nastavení povoleno
- Režim schválení správce pro integrovaný účet správce
 - Povoluje Režim schválení správce pro uživatele Administrator
 - Účet Administrator je ve výchozím nastavení zakázán
 - Ve výchozím nastavení zakázáno (tedy automatické zvyšování oprávnění bez jakékoliv výzvy)

Zásady ovlivňující chování UAC (4)

- Spustit všechny správce v Režimu schválení správce
 - Zakázáním dojde k vypnutí UAC pro všechny správce
 - Ve výchozím nastavení povoleno
- Virtualizovat chyby zápisu do souboru a registru do umístění jednotlivých uživatelů
 - Povolení povolí přesměrování zápisů do chráněných adresářů a registrů do profilu uživatele
 - Ve výchozím nastavení povoleno
- Zjistit instalace aplikací a zobrazit výzvu ke zvýšení oprávnění (ve výchozím nastavení povoleno)
 - Umožňuje instalátorům aplikací požadovat zvýšení oprávnění

Zásady ovlivňující chování UAC (5)

- Zvýšit oprávnění pouze u aplikací UIAccess, které jsou nainstalovány v zabezpečených umístěních
 - Zakázání umožňuje každé aplikaci požadovat spuštění s úrovní integrity UIAccess (aplikace musí být ovšem pořád podepsána důvěryhodnou certifikační autoritou)
 - Výchozí nastavení je povoleno
- Zvýšit oprávnění pouze u podepsaných a ověřených spustitelných souborů
 - Všechny nepodepsané aplikace, případně aplikace podepsané nedůvěryhodným vydavatelem, nemůžou vyžadovat zvyšování oprávnění (automaticky zamítnuto)
 - Ve výchozím nastavení zakázáno

Autentizace a autorizace

Základní pojmy

- Autentizace (*authentication*)
 - Ověření identity uživatele důvěryhodnou autoritou (lokální bezpečnostní autoritou (LSA, *Local Security Authority*), řadičem domény, ...)
 - Vytváří se tzv. přístupový token (*access token*)
- Autorizace (*authorization*)
 - Prokázání identity uživatele pro zpřístupnění určitého prostředku (souboru, adresáře, tiskárny, ...)
 - Ověření oprávnění uživatele resp. skupin uložených v předloženém přístupovém tokenu

Správce pověření

- Uchovává přihlašovací jména a hesla pro přístup k síťovým prostředkům (a webovým stránkám)
 - Uloženy v trezoru Windows (*Windows Vault*)
 - Hesla nelze zobrazit
- Možnost zálohování / obnovy
 - Migrace uložených pověření na jiný počítač
 - Zálohuje i některé certifikáty (ne certifikáty pro EFS)
 - Záloha chráněná heslem
 - Zálohování i obnova vždy přes zabezpečenou plochu

Spouštění programů pod jiným účtem

- Nástroj **runas** [/profile | /noprofile] [/savecred | /smartcard] /user:<jméno> "<program>"
- Spuštěný program běží pod zadaným uživatelem
 - Přístup k prostředkům realizován tímto uživatelem
- Možnost načtení / nenačtení profilu uživatele
 - Při načtení lze přistupovat k šifrovaným datům (EFS) daného uživatele (certifikáty jsou uloženy v profilu)
 - Nenačtení profilu urychluje spuštění programu, ale program nemusí pracovat správně

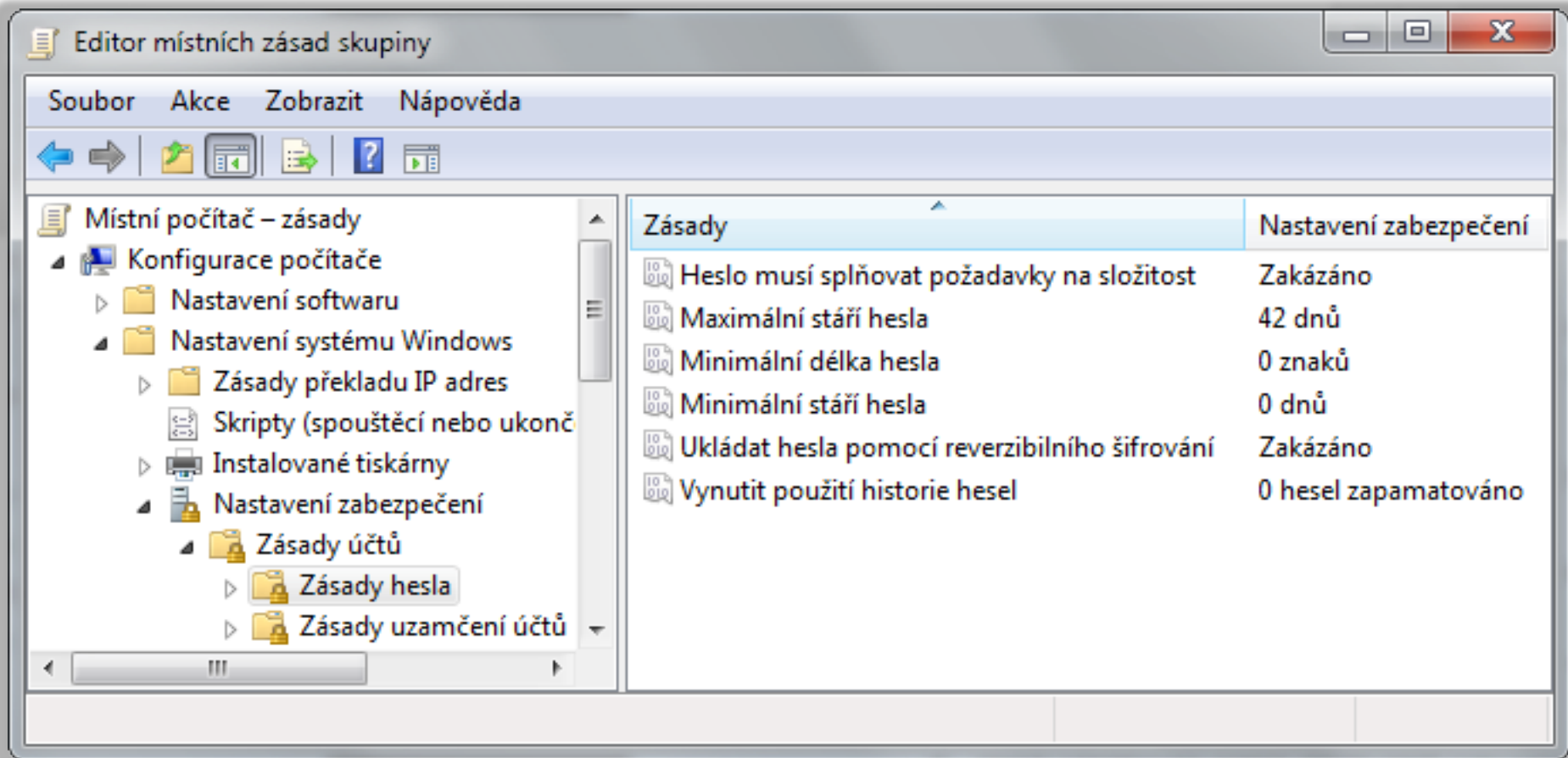
Pověření a oprávnění

- Zadané pověření lze uložit v trezoru Windows
 - Přepínač **/savecred** pro uložení i použití pověření
- Pověření lze dodat na čipové kartě (*smart card*)
 - Přepínač **/smartcard** (nelze uložit přes **/savecred**)
- Všechny spouštěné programy běží s oprávněními standardního uživatele
 - Nelze zobrazovat výzvy k zadání souhlasu / pověření
 - Není možné provést zvýšení oprávnění jinak než plně automaticky

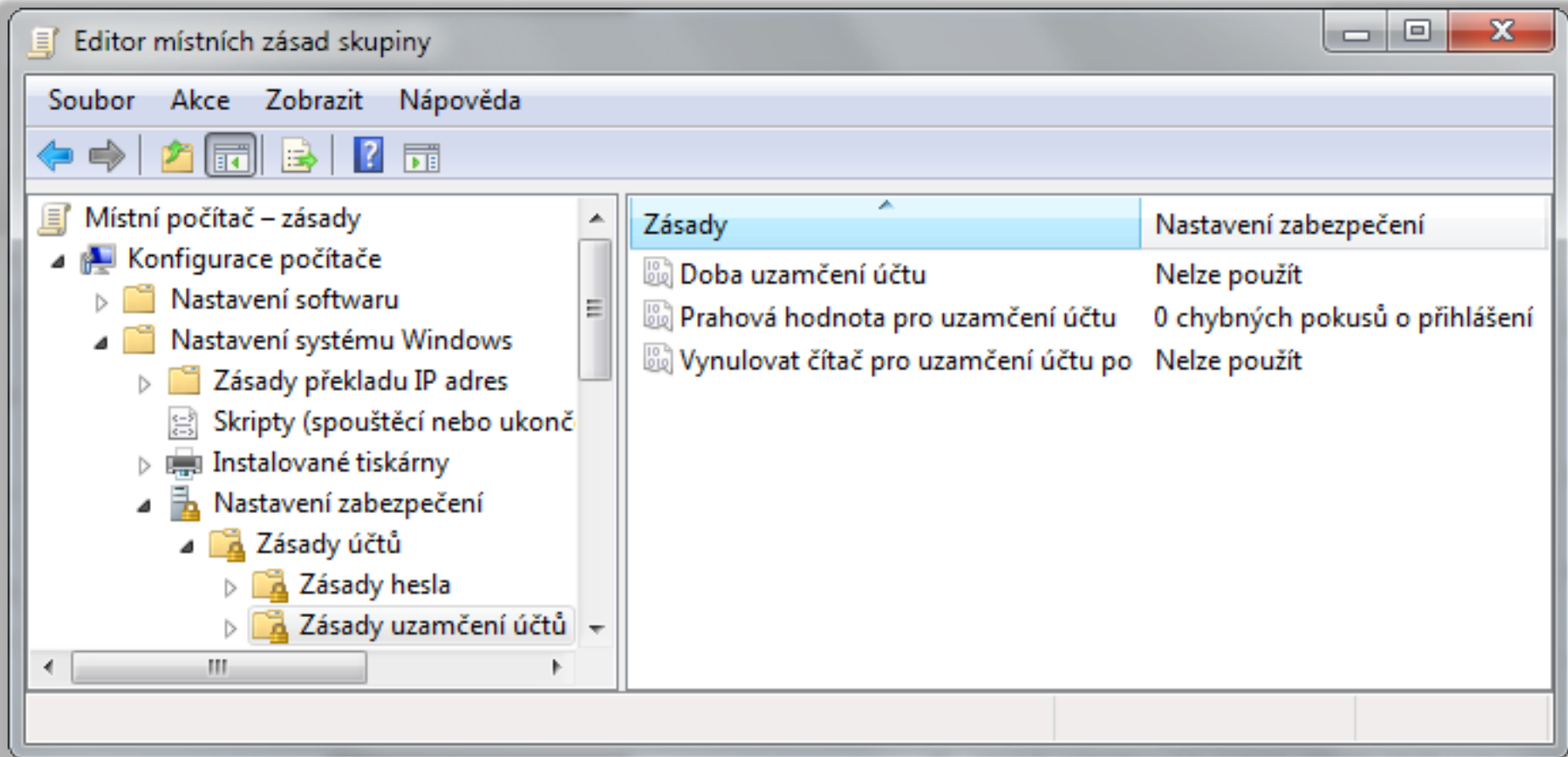
Vícefaktorová autentizace

- Autentizace za pomoci dvou nebo více rozdílných metod (vícenásobné ověření)
 - Výrazně zvyšuje bezpečnost
- Možnosti autentizace v systémech Windows
 - Zadáním pověření (jména a hesla)
 - Čipovou kartou (*smart card*)
 - Biometrickým identifikátorem (*Biometric ID*)
 - Jakýmkoliv vlastním způsobem vytvořením vlastního poskytovatele pověření (*Credential Provider*)

Zásady hesel



Zásady uzamčení účtů



Možnosti řešení zapomenutí hesla

- Použití diskety pro resetování hesla uživatelem
 - Data pro resetování hesla uložena na disketě nebo USB úložném zařízení (v nechráněné podobě)
 - Zachování všech osobních certifikátů (včetně EFS certifikátů) a hesel uložených v trezoru Windows
- Resetování hesla správcem
 - Ztráta osobních certifikátů (včetně EFS certifikátů) a hesel uložených v trezoru Windows

Zálohování EFS certifikátů

- Export do **.pfx** souboru
 - Chráněn heslem
 - Obsahuje veřejný i privátní klíč
- 3 možnosti exportu
 - Přes průvodce Spravovat šifrovací certifikáty souborů
 - Přes MMC konzoli Certifikáty (**certmgr.msc**)
 - Příkazem **cipher /x <název>**

Čipové karty

- Obsahují certifikáty použitelné pro autentizaci
 - Možnost zneplatnění (*revoke*) certifikátu při odcizení
- Nativní podpora (ovladače) v systému Windows
- Jednoduchá integrace do **Active Directory**
- Nastavení přes zásady skupiny
 - Možnosti zabezpečení, část Interaktivní přihlašování

Zásady čipových karet

- Požadovat čipovou kartu
 - Při povolení se není možné autentizovat bez použití čipové karty
 - Ve výchozím nastavení zakázáno
- Chování při odebrání čipové karty
 - Žádná akce (výchozí nastavení)
 - Uzamknout pracovní stanici
 - Vynutit odhlášení
 - Odpojit v případě relace Vzdálené plochy

Omezování aplikací

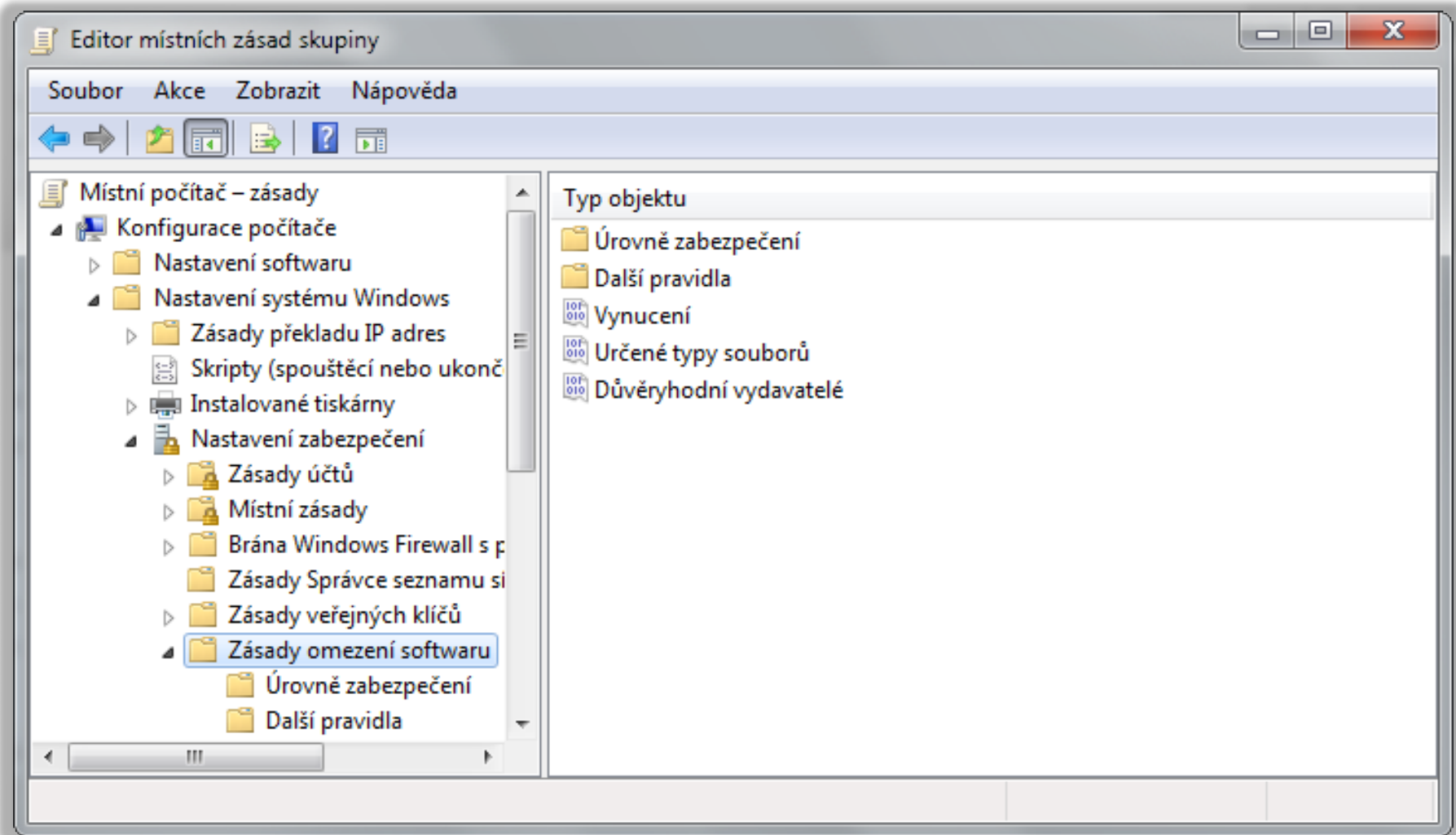
Zásady omezení softwaru

- Podpora od Windows XP a Windows Server 2003
- Celkem 5 různých typů pravidel (podle priority)
 - 1) Pravidla algoritmu hash
 - 2) Pravidla certifikátu
 - 3) Pravidla cesty
 - 4) Pravidla zóny sítě
 - 5) Výchozí pravidla
- Priorita podle specifičnosti pravidel
 - Více specifická pravidla mají vždy vyšší prioritu

Výchozí pravidla

- Vždy může být aktivní pouze jedno
 - Výběr pod uzlem Úrovně zabezpečení
- Celkem 3 výchozí pravidla
 - Nepovoleno
 - Aplikace, jenž nejsou explicitně povoleny nesmí běžet
 - Standardní uživatel
 - Aplikace, jenž nevyžadují oprávnění správce mohou běžet
 - Bez omezení
 - Aplikace, jenž nejsou explicitně zakázány mohou běžet

Nastavení v zásadách skupiny



Pravidla cesty

- Umožňují specifikovat soubory, adresáře či klíče registru (cesty ke klíčům registru)
 - Podpora zástupných znaků * a ?
 - Podpora systémových proměnných (%**SystemRoot**%)
 - Klíče registru musí být uzavřeny mezi znaky %
- Závislé na umístění souboru
 - Lze obejít přesunutím (přejmenováním) souboru
- Pravidla obsahující více specifickou cestu mají vždy vyšší prioritu

Pravidla algoritmu hash

- Umožňují specifikovat pouze soubory
- Generování digitálního otisku (*hash*) souboru
 - Generován na základě binárního obsahu
 - Unikátní pro každý soubor (i pro každou jeho verzi)
 - Mění se při jakékoliv změně souboru
- Potřeba úpravy při každé aktualizaci souboru
- Nezávislost na umístění souboru

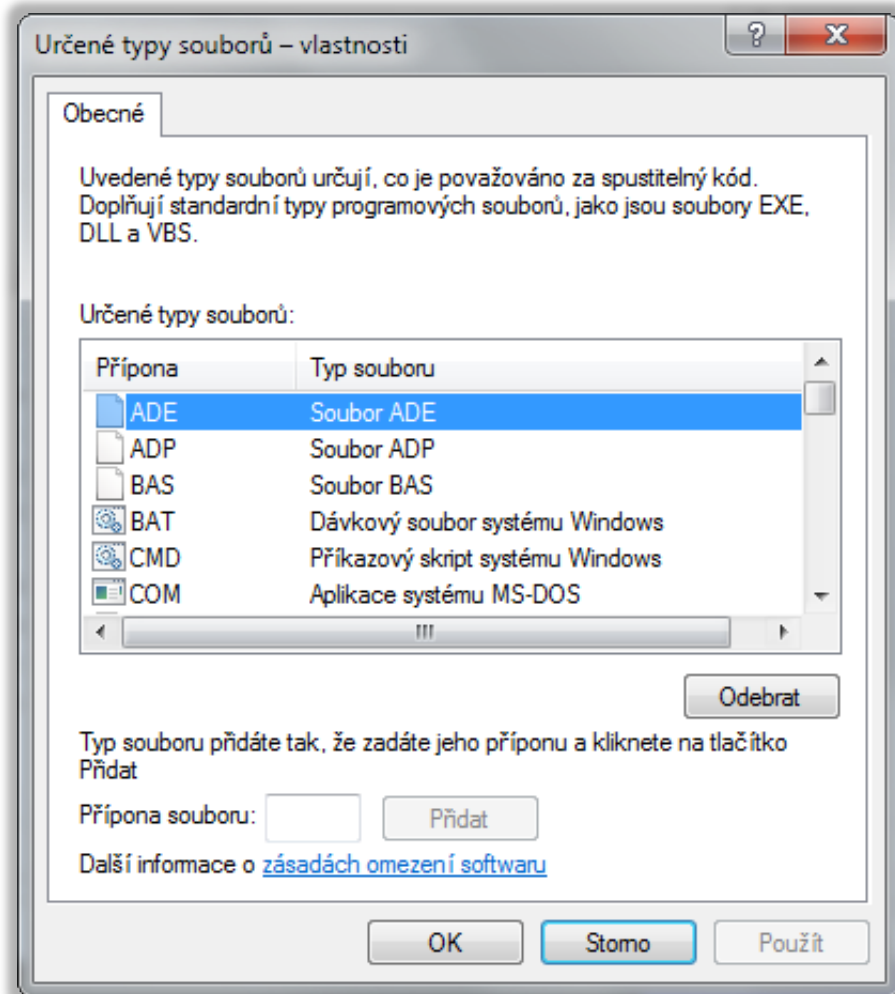
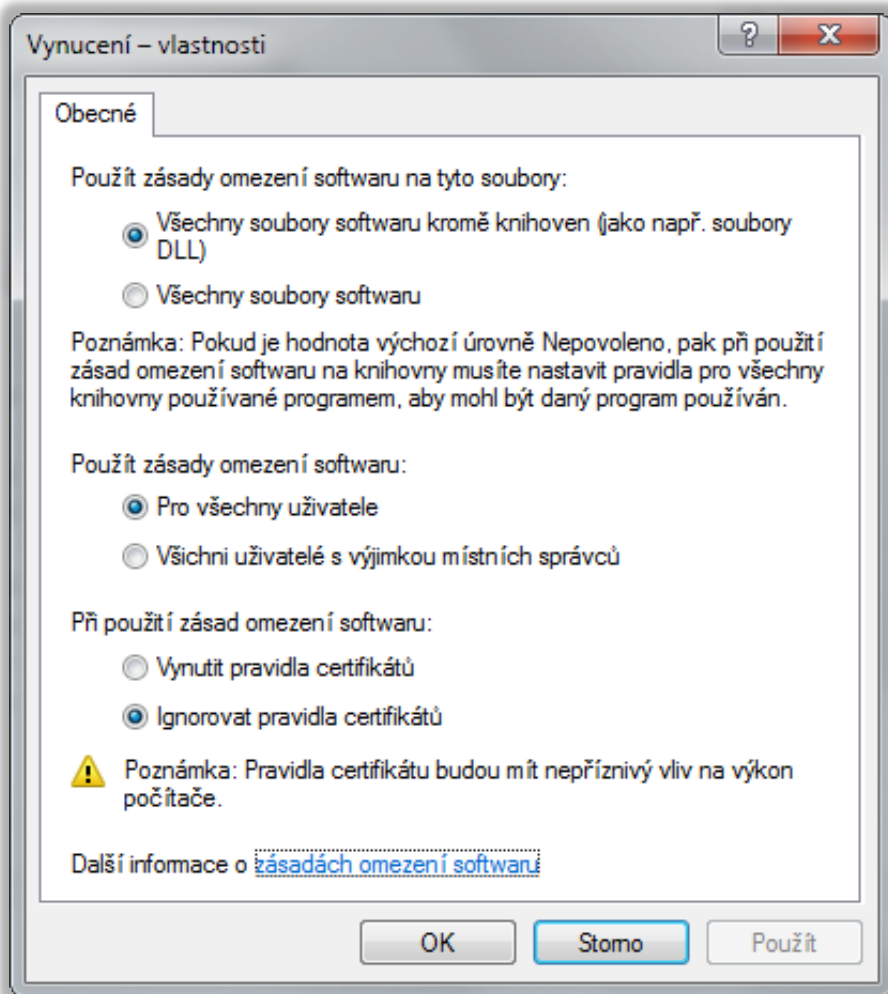
Pravidla certifikátu

- Umožňují specifikovat pouze certifikáty
 - Identifikují soubory podepsané zadaným certifikátem
- Nezávislost na umístění souboru
- Žádná potřeba úpravy při aktualizaci souboru
 - Soubor je pořád podepsán stejným certifikátem
- Nutnost ověřování validity certifikátu
 - Vyšší zatížení počítače
- Aplikovány na všechny soubory daného výrobce
- Musí být explicitně povoleny

Pravidla zóny sítě

- Umožňují specifikovat jen **.msi** soubory získané přes Internet Explorer
- Omezování spouštění **.msi** souborů na základě typu sítě, z níž byly získány
 - Důvěryhodné servery
 - Internet
 - Místní intranet
 - Místní počítač
 - Servery s omezeným přístupem

Vynucení a určené typy souborů



AppLocker

- K dispozici jen v edicích Enterprise a Ultimate
 - Podpora od Windows 7 a Windows Server 2008 R2
- Pro správné fungování musí běžet služba Identita Aplikace (AIS, *Application Identity Service*)
 - Ve výchozím nastavení neběží (ruční start)
- Omezování běhu aplikací pro jednotlivé uživatele nebo skupiny
- Podpora automatického vytváření pravidel
 - Průvodce pro analýzu adresářů a generování pravidel

Typy pravidel

- Pravidla vydavatele
 - Pracují s certifikáty (digitálně podepsané soubory)
 - Lze rozlišovat na úrovni vydavatele, názvu produktu, názvu souboru nebo verze souboru (<, >, =)
- Pravidla hodnoty hash souboru
 - Možnost počítat hodnotu hash pro všechny soubory v zadaném adresáři
- Pravidla cesty
 - Nelze definovat systémové proměnné (jen proměnné AppLocker) ani cesty ke klíčům registru

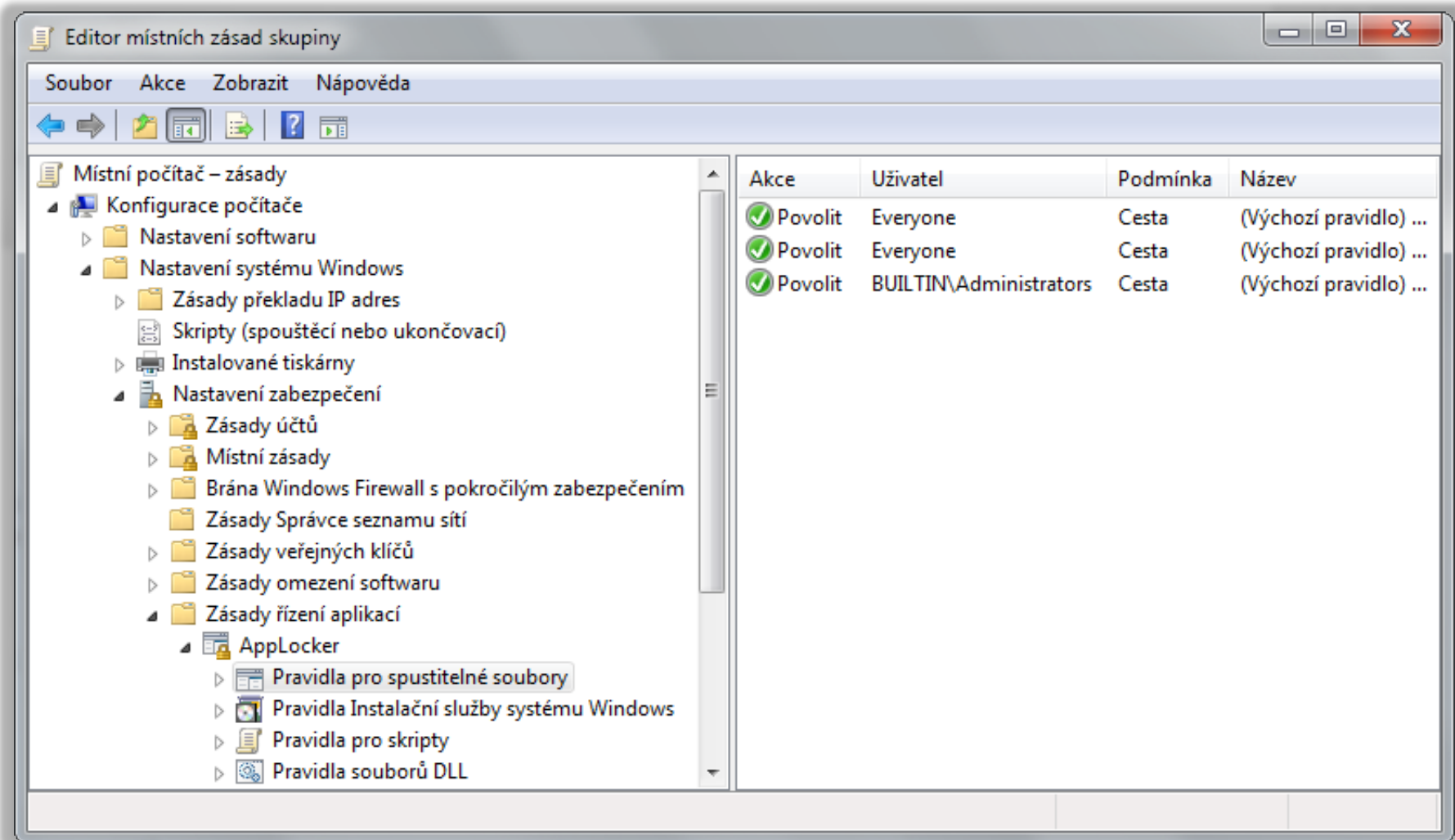
Kolekce pravidel

- Pravidla pro spustitelné soubory
 - Aplikace na soubory s příponami **.exe** a **.com**
- Pravidla Instalační služby systému Windows
 - Aplikace na soubory s příponami **.msi** a **.msp**
- Pravidla pro skripty
 - Soubory s příponami **.ps1**, **.bat**, **.cmd**, **.vbs** a **.js**
- Pravidla souborů DLL
 - Soubory s příponami **.dll** a **.ocx**
 - Musí být explicitně povoleny

Výchozí pravidla

- Je možné generovat automaticky pro jednotlivé typy (kolekce) souborů
- Povolují spouštění souborů kdekoliv pro správce
- Pro spustitelné soubory, skripty a soubory DLL
 - Povolují spouštění souborů obsažených v adresářích **Windows** a **Program Files** pro všechny uživatele
- Pro soubory Instalační služby systému Windows
 - Povolují spouštění souborů obsažených v adresáři **Windows\Installer** a všech digitálně podepsaných souborů kdekoliv pro všechny uživatele

Nastavení v zásadách skupiny



Priorita pravidel a výjimky

- 1) Blokující pravidla (akce Odepřít)
- 2) Povolující pravidla (akce Povolit)
- 3) Integrované blokující pravidlo
 - Nelze změnit
 - Blokuje spouštění všech souborů
- Výjimky z pravidel
 - Mohou být ve formě pravidla vydavatele, cesty i hash
 - Lze definovat pro blokující i povolující pravidla
 - Lze definovat jen u pravidel vydavatele a cesty

Auditování

- Monitorování aplikace AppLocker pravidel
 - Informace uloženy v protokolu AppLocker (Protokoly aplikací a služeb | Microsoft | Windows)
- Ukládají se informace
 - Název pravidla
 - SID cílového uživatele nebo skupiny
 - Cesta k souboru
 - Akce (spuštění povoleno nebo odepřeno)
 - Typ pravidla (vydavatel, hodnota hash, cesta)

Nastavení auditování a povolení DLL

