KAPITOLA 5

Zvýšení zabezpečení počítače

V této kapitole:

Zdá se, že bezpečnostní postupy a nastavení jsou nezbytné pro úspěšnou správu systémů. Dvěma klíčovými způsoby konfigurace nastavení zabezpečení jsou použití šablon zabezpečení a použití zásad zabezpečení. Obě tyto funkce spravují nastavení systému, které byste typicky jinak spravovali prostřednictvím Zásad skupiny (Group Policy).

Použití šablon zabezpečení

Šablony zabezpečení nabízí centralizovaný způsob správy nastavení souvisejících se zabezpečením pracovních stanic a serverů. Šablony zabezpečení použijte při aplikaci vlastních množin definicí Zásad skupiny (Group Policy), které souvisí se zabezpečením příslušného počítače.

Tyto definice zásad obecně ovlivňují následující zásady:

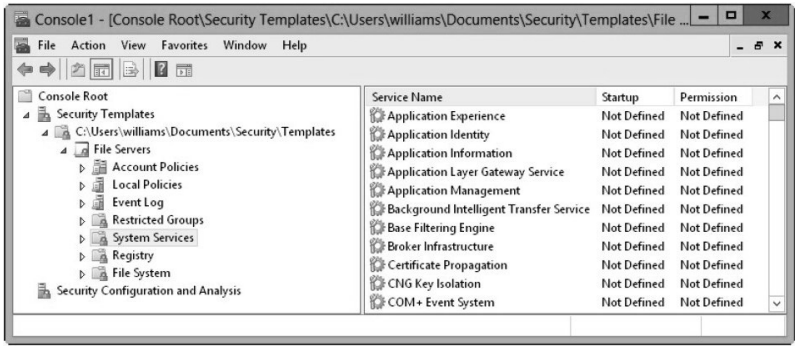
- **Zásady účtů** (Account Policies) – řídí zabezpečení hesel, uzamčení účtů a bezpečnostní protokol Kerberos
- **Místní zásady (Local Policies)** – řídí zabezpečení auditování, přiřazení uživatelských práv a dalších možností zabezpečení
- **Zásady protokolu událostí (Event Log)** – řídí zabezpečení protokolování událostí
- **Zásady skupin s omezeným členstvím (Restricted Groups)** – řídí zabezpečení správy členství místních skupin
- **Zásady systémových služeb (Systém Services)** – řídí zabezpečení a režim spouštění místních služeb
- **Zásady systému souborů (File System)** – řídí zabezpečení cest k souborům a složkám v místním systému souborů
- **Zásady registru (Registry Policies)** – řídí zabezpečení oprávnění klíčů registru souvisejících se zabezpečením

Poznámka: Šablony zabezpečení jsou dostupné ve všech instalacích systému Microsoft Windows Server a lze je importovat do libovolných objektů zásad skupin. Šablony zabezpečení se aplikují pouze na oblast Nastavení počítače (Computer Configuration) nástroje Zásad skupiny (Group Policy). Neaplikují se na oblast Nastavení počítače (User Configuration) nástroje Zásad skupiny (Group Policy). V nástroji Zásady skupiny (Group Policy) najdete všechna použitelná nastavení v části Nastavení počítače\Nastavení systému Windows\Nastavení zabezpečení (Computer Configuration\Windows Settings\Security Settings). Některá nastavení zabezpečení nejsou obsažena, například ta, která se aplikují na bezdrátové sítě, veřejné klíče, omezení softwaru a zabezpečení protokolu IP.

Práce se šablonami zabezpečení sestává z několika kroků:

1. Při vytváření nové šablony použijte modul snap-in Šablony zabezpečení. Případně zvolte již existující šablonu a upravte ji.
2. Prostřednictvím modulu snap-in Šablony zabezpečení proveďte nezbytné úpravy nastavení šablony a změny uložte.
3. Pomocí modulu snap-in Konfigurace a analýza zabezpečení můžete analyzovat rozdíly mezi šablonou, s níž právě pracujete, a aktuálním nastavením zabezpečení počítače.
4. Jakmile zjistíte rozdíly mezi nastaveními šablony a aktuálními nastaveními počítače, zrevidujte šablonu.
5. Použijte na šablonu modul snap-in Konfigurace a analýza zabezpečení, čímž přepíšete stávající nastavení zabezpečení.

Při prvním použití šablon zabezpečení byste měli zjistit, zda můžete vycházet z nějakých existujících šablon. Ty mohou být dílem některých jiných správců. Případně může mít základní (směrné) šablony v databázi firma. Začít však můžete i tvorbou vlastní šablony, viz obrázek 5.1.



Obrázek 5.1: Prohlížet si a vytvářet šablony zabezpečení můžete pomocí modulu snap-in Šablony zabezpečení

Tip: Jakmile si zvolíte šablonu, na níž začnete pracovat, měli byste si projít nastavení, které šablona aplikuje, a zjistit, jaký dopad bude mít takové nastavení na vaše prostředí. Pokud se vám nehodí, měli byste ho vhodně upravit anebo odstranit.

Šablony neaplikujeme modulem snap-in Šablony zabezpečení, nýbrž modulem snap-in Konfigurace a analýza zabezpečení. Tentýž modul můžete použít i tehdy, když budete chtít porovnat nastavení šablony a aktuální nastavení počítače. Místa, v nichž se aktuální nastavení neshoduje s nastavením šablony, budou ve výsledcích zvýrazněna. Snadno tak zjistíte, zda nedošlo ke změně nastavení zabezpečení.

Použití modulů snap-in Šablony zabezpečení (Security Templates) a Konfigurace a analýza zabezpečení (Security Configuration And Analysis)

Moduly snap-in týkající se zabezpečení můžete otevřít pomocí následujících kroků:

1. Spusťte konzoli MMC (Microsoft Management Console). Jedním ze způsobů, jak to provést, je stisknout klávesu Windows, zadat příkaz **mmc** a poté stisknout klávesu Enter.
2. V konzoli Microsoft Management Console klepněte na příkaz Soubor (File) a poté na Přidat nebo odebrat modul snap-in (Add/Remove Snap-In).
3. V dialogu Přidat nebo odebrat modul snap-in (Add Or Remove Snap-Ins) klepněte na položku Šablony zabezpečení (Security Templates) a poté na tlačítko Přidat (Add).
4. Klepněte na položku Konfigurace a analýza zabezpečení (Security Configuration And Analysis) a poté na tlačítko Přidat (Add). Klepněte na tlačítko OK.

Standardně modul snap-in Šablony zabezpečení (Security Templates) hledá šablony zabezpečení ve složce %SystemDrive%\Users\%UserName%\Documents\Security\Templates. Další cesty pro vyhledávání šablon můžete přidat pomocí následujících kroků:

1. V modulu snap-in Šablony zabezpečení (Security Templates), který jste vybrali v konzoli MMC, zvolte v nabídce Akce (Action) příkaz Nová cesta hledání šablony (New Template Search Path).
2. V dialogovém okně Vyhledat složku vyberte umístění šablon, které chcete přidat, například %SystemRoot%\Security\Policies. Klepněte na tlačítko OK.

   Teď, když jste vybrali cestu pro vyhledávání šablon, se kterou chcete pracovat, můžete vybrat šablonu a rozbalit příslušné poznámky, abyste zkontrolovali její nastavení.

Novou šablonu můžete vytvořit pomocí následujících kroků:

1. V modulu snap-in Šablony zabezpečení (Security Templates) dlouze stiskněte cestu pro vyhledávání, v níž chcete vytvořit novou šablonu, či na ni klepněte pravým tlačítkem myši a poté zvolte příkaz Nová šablona (New Template).
2. Zadejte název a popis šablony v zobrazeném dialogu.
3. Klepnutím na tlačítko OK vytvořte šablonu. Šablona nebude obsahovat žádná nakonfigurovaná nastavení, takže budete muset nastavení pečlivě změnit předtím, než bude šablona připravena k použití.
4. Jakmile šablonu upravíte, uložte změny dlouhým stisknutím či klepnutím pravým tlačítkem myši na šablonu v modulu snap-in Šablona zabezpečení a výběrem volby Uložit. Pokud chcete šablonu uložit pod jiným názvem, můžete rovněž použít možnost Uložit jako.

Kontrola a změna nastavení šablon

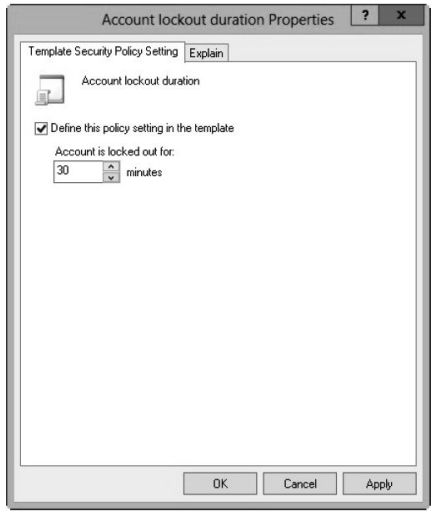
Následující části popisují způsob práce s nastaveními šablon. Jak již víte, každý typ nastavení šablon spravujete trošku odlišným způsobem.

Změna nastavení zásad účtů, místních nastavení a nastavení protokolu událostí

Nastavení zásad účtů řídí zabezpečení hesel, uzamčení účtů a protokol Kerberos. Nastavení místních zásad řídí zabezpečení auditování, přiřazení uživatelských práv a dalších možností zabezpečení. Nastavení zásad protokolování událostí řídí zabezpečení protokolování událostí. Podrobné informace o nastaveních zásad účtů a místních zásad najdete v kapitole 8, „Vytváření uživatelských a skupinových účtů". Podrobné informace o konfiguraci protokolování událostí najdete v kapitole 3, „Monitorování procesů, služeb a událostí".

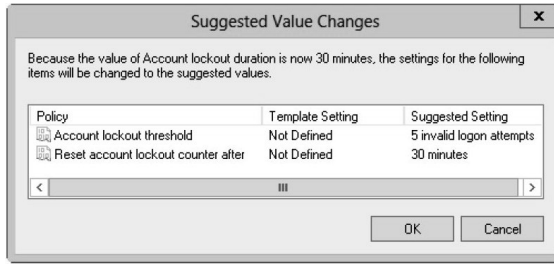
U zásad účtů, místních zásad a zásad protokolu událostí můžete změnit nastavení šablony pomocí následujících kroků:

1. V modulu snap-in Šablony zabezpečení (Security Templates) rozbalte uzel Zásady účtů (Account Policies) nebo Místní zásady (Local Policies) podle potřeby a poté vyberte odpovídající poduzel, třeba Zásady hesla (Password Policy) nebo Zásady uzamčení účtů (Account Lockout Policy).
2. V podokně vpravo jsou abecedně podle názvu vypsána nastavení zásad. Hodnota ve sloupci Nastavení počítače (Computer Settings) znázorňuje aktuální nastavení. Pokud šablona změní nastavení tak, že již nadále není definováno, hodnota je uvedena jako Nedefinováno (Not Defined).
3. Poklepáním na nastavení zobrazte dialog Vlastnosti (Properties), viz obrázek 5.2. Pro zjištění důvodu nastavení klepněte na kartu Vysvětlit (Explain). Pro definici a použití nastavení zásady zaškrtněte políčko Definovat v šabloně toto nastavení zásad (Define This Policy Setting In The Template). Pro zrušení této zásady a její nepoužití zrušte zaškrtnutí tohoto políčka.



Obrázek 5.2: Změna nastavení šablony pro zásady účtů a místní zásady

4. Pokud jste povolili nastavení zásad, konfigurací dalších možností přesně specifikujte, jak se má dané nastavení zásad použít.
5. Klepnutím na tlačítko OK uložte změny nastavení. Může se zobrazit dialog Navrhované změny hodnot (Suggested Value Changes), viz obrázek 5.3. Tento dialog vás informuje o všech dalších hodnotách, které se změní na navržené hodnoty vlivem vaší změny nastavení. Například když změníte nastavení Prahová změna pro uzamčení účtu (Account Lockout Threshold), systém Windows může rovněž změnit nastavení Doba uzamčení účtu (Account Lockout Duration) a Vynulovat čítač pro uzamčení účtu po (Reset Account Lockout Counter After), viz obrázek.



Obrázek 5.3: Kontrola změn navržených hodnot

Konfigurace skupin s omezeným členstvím

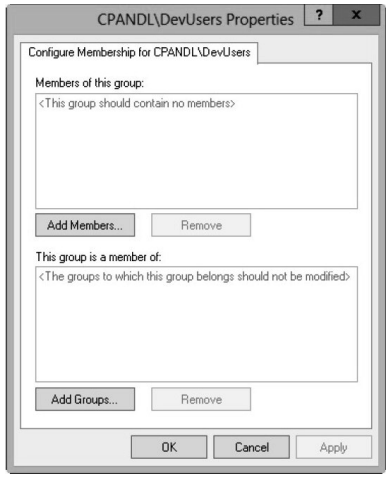
Nastavení zásad skupin s omezeným členstvím řídí seznam členů skupin, stejně jako skupin, do kterých patří konfigurovaná skupina. Členství skupiny můžete omezit pomocí následujících kroků:

1. V modulu snap-in Šablony zabezpečení (Security Templates) vyberte uzel Skupiny s omezeným členstvím (Restricted Groups). V podokně vpravo jsou abecedně podle názvu vypsány aktuální skupiny s omezeným členstvím. Členové skupiny jsou rovněž vypsáni stejně tak skupiny, jichž je skupina s omezeným členstvím členem.
2. Skupinu s omezeným členstvím můžete přidat dlouhým stisknutím či klepnutím pravým tlačítkem myši na uzel Skupiny s omezeným členstvím (Restricted Groups) v levém podokně a poté výběrem příkazu Přidat skupinu (Add Group). V dialogu Přidat skupinu (Add Group) klepněte na tlačítko Procházet (Browse).
3. V dialogovém okně Vyberte objekt typu: skupina (Select Groups) zadejte název skupiny, jejíž členství chcete omezit, a poté klepněte na tlačítko Kontrola názvů (Check Names). Pokud se nalezne více shod, vyberte účet, který chcete použít, a poté klepněte na tlačítko OK. Pokud nejsou nelezeny žádné shody, aktualizujte zadaný název a zkuste vyhledávat znovu. Tento krok zopakujte podle potřeby a poté klepněte na tlačítko OK.
4. V dialogovém okně Vlastnosti (Properties), viz obrázek 5.4, můžete použít možnost Přidat členy (Add Members) pro přidání členů do skupiny. Klepněte na příkaz Přidat členy (Add Members) a poté zadejte členy skupiny. Pokud skupina nemá mít žádné členy, odeberte všechny členy klepnutím na tlačítko Remove. Všichni členové, kteří nejsou specifikováni v nastavení zásad skupiny s omezeným členstvím, jsou při použití šablony zabezpečení odebráni.
5. V dialogovém okně Vlastnosti (Properties) klepněte na tlačítko Přidat skupinu (Add Groups), abyste specifikovali skupiny, do nichž tato skupina patří. Pokud specifikujete členství ve skupinách, skupiny, do nichž tato skupina patří, jsou vypsány přesně tak, jak jste je použili (za předpokladu, že jsou skupiny platné v použitelné pracovní skupině nebo doméně). Pokud nespecifikujete členství ve skupinách, skupiny, do nichž tato skupina patří, se při použití šablony nezmění.
6. Klepnutím na tlačítko OK nastavení uložte.

Odebrat omezení členství skupiny můžete pomocí následujících kroků:

1. V modulu snap-in Šablony zabezpečení (Security Templates) vyberte uzel Skupiny s omezeným členstvím (Restricted Groups). V podokně vpravo jsou abecedně podle názvu vypsány aktuální skupiny s omezeným členstvím. Členové skupiny jsou vypsáni společně se skupinami, jichž je daná skupina s omezeným členstvím členem.

2. Dlouze stiskněte skupinu, jejíž členství by nemělo být omezeno, či na ni klepněte pravým tlačítkem myši a poté zvolte příkaz Odebrat (Delete). Po výzvě k potvrzení akce klepněte na tlačítko Ano (Yes).

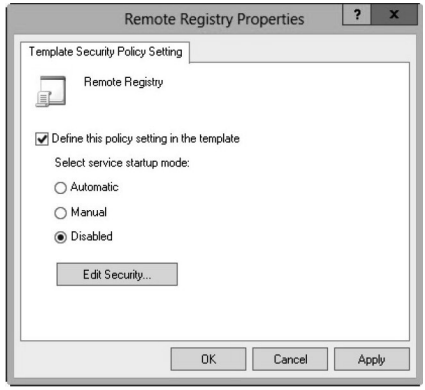


Obrázek 5.4: Zkontrolujte si navržené změny hodnot

Povolení, zakázání a konfigurace systémových služeb

Nastavení zásad systémových služeb řídí obecné zabezpečení a režim spouštění místních služeb. Systémové služby můžete povolit, zakázat a konfigurovat pomocí následujících kroků:

1. V modulu snap-in Šablony zabezpečení (Security Templates) vyberte uzel Systémové služby (System Services). V podokně vpravo jsou abecedně podle názvu, nastavení spouštění a konfigurace oprávnění vypsány aktuálně nainstalované služby na počítači, s nímž pracujete. Při práci se systémovými službami mějte na paměti následující skutečnosti:
   - Pokud šablona nezmění konfiguraci spouštění služby, hodnota sloupce Po spuštění (Startup) je uvedena jako Nedefinováno (Not Defined). Jinak je konfigurace spouštění uvedena jako jedna z následujících hodnot: Automaticky (Automatic), Ručně (Manual) nebo Zakázat (Disabled).
   - Pokud šablona nemění konfiguraci zabezpečení služby, hodnota sloupce oprávnění (Permission) je uvedena jako Nedefinováno (Not Defined). Jinak je konfigurace zabezpečení uvedena jako Nakonfigurováno (Configured).
2. Poklepejte na položku systémové služby, abyste zobrazili její dialogové okno Vlastnosti (Properties), jež je zobrazené na obrázku 5.4. Pro definici a použití nastavení zásad zaškrtněte políčko Definovat v šabloně toto nastavení zásad (Define This Policy Setting In The Template). Pro odstranění této zásady a její nepoužití zrušte zaškrtnutí tohoto políčka.



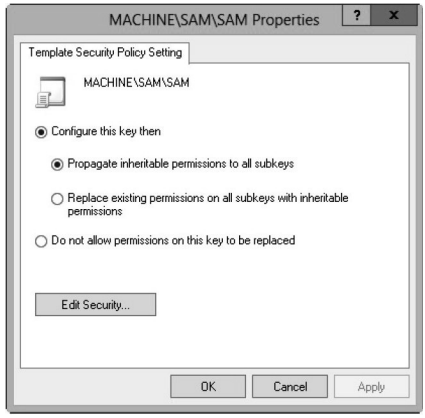
Obrázek 5.5: Změna nastavení šablony pro systémové služby

3. Pokud jste zapnuli nastavení zásad, specifikujte režim spouštění služby výběrem možností Automaticky (Automatic), Ručně (Manual) nebo Zakázat (Disabled). Mějte na paměti následující:
   - Možnost Automaticky (Automatic) zajistí, že se služba automaticky spustí po spuštění operačního systému. Toto nastavení zvolte u základních služeb, o nichž víte, že jsou bezpečné, a u nichž chcete zajistit spuštění, pokud jsou nainstalovány na počítači, na který je použita rovněž šablona.
   - Možnost Ručně (Manual) zabraňuje automatickému spuštění služeb a povolí pouze ruční spuštění služby (uživatelem, aplikací či jinou službou). Toto nastavení zvolte, chcete-li omezit nepodstatné nebo nepoužívané služby nebo když chcete omezit služby, o nichž víte, že nejsou zcela bezpečné.
   - Možnost Zakázat (Disabled) zabraňuje automatickému i ručnímu spuštění služby. Toto nastavení zvolte pouze v případě nepotřebných nebo nepoužívaných služeb, jejichž spuštění chcete zabránit.
4. Pokud znáte konfiguraci zabezpečení, kterou by měla daná služba použít, klepněte na příkaz Upravit zabezpečení (Edit Security) a poté nastavte oprávnění služby v dialogovém okně Zabezpečení pro (Security For). Můžete natavit oprávnění umožňující konkrétním uživatelům a skupinám spouštět, zastavovat a pozastavovat službu na daném počítači.
5. Klepněte na tlačítko OK.

Konfigurace nastavení zabezpečení cest k registru a systému souborů

Nastavení zásad systému souborů řídí zabezpečení cest k souborům a složkám v místním systému souborů. Nastavení zásad registru řídí hodnoty klíčů registru souvisejících se zabezpečením. Zobrazit nebo změnit nastavení zabezpečení aktuálně definovaných cest k registru a systému souborů můžete pomocí následujících kroků:

1. V modulu snap-in Šablony zabezpečení (Security Templates) vyberte uzel Registry nebo uzel Systém souborů (File System), podle toho, s jakým typem cest chcete pracovat. V podokně vpravo jsou abecedně podle názvu vypsány aktuálně zabezpečené cesty.
2. Myší poklepejte na cestě k registru nebo souboru, abyste zobrazili její aktuální nastavení, viz obrázek 5.6.

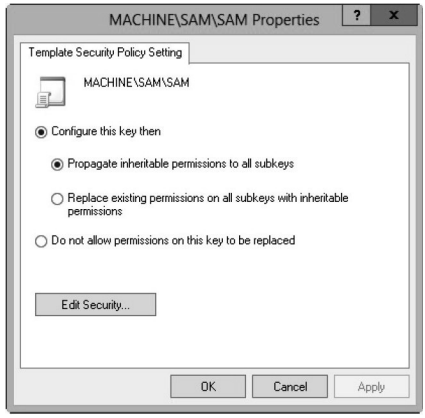


Obrázek 5.6: Změna nastavení šablony cestám a klíčům

3. Abyste zaručili, že nedojde k odebrání oprávnění k cestě nebo klíči, zvolte možnost Zakázat tomuto souboru nebo složce (Do Not Allow Permissions On This Key To Be Replaced) a poté klepněte na tlačítko OK. Ostatní kroky postupu přeskočte.
4. Pro konfiguraci cesty nebo klíče a odebrání oprávnění zvolte možnost Nakonfigurovat tento soubor či složku a provést následující akci (Configure This Key Then) a poté zvolte jednu z následujících možností:
   - **Šířit dědičná oprávnění na všechny soubory a složky (Propagate Inheritable Permissions To All Subkeys)** – tuto možnost zvolte tehdy, chcete-li pro tuto cestu k registru nebo souboru a všechny cesty k registru a souboru pod touto cestou použít všechna oprávnění, která lze zdědit. Existující oprávnění se nahradí pouze tehdy, pokud odporují nastavením oprávnění zabezpečení pro tuto cestu.
   - **Nahradit existují oprávnění ke všem souborům a podsložkám dědičnými oprávněními (Replace Existing Permissions On All Subkeys With Inheritable Permissions)** – tuto možnost zvolte pro nahrazení všech existujících oprávnění pro cestu k registru nebo souboru a pro všechny cesty k registru a souboru pod touto cestou. Všechna existující oprávnění se nahradí a zůstanou pouze aktuální oprávnění.
5. Klepněte na tlačítko Upravit zabezpečení (Edit Security). V dialogovém okně Databaze zabezpečení pro (Security For) nakonfigurujte požadovaná oprá-

není zabezpečení pro uživatele a skupiny. K dispozici máte stejné možnosti pro oprávnění, auditování a vlastnictví, a to pro soubory a složky použité se systémem souborů NTFS. Další podrobnosti o oprávnění, auditování a vlastnictví najdete v kapitole 12, „Sdílení, zabezpečení a auditování dat".

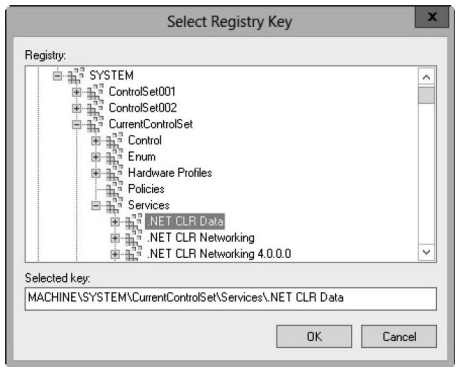
6. Dvojím klepnutím na tlačítko OK uložte nastavení.



Obrázek 5.6: Změna nastavení šablony pro cesty a klíče

Nastavení zabezpečení pro cesty k registru můžete definovat pomocí následujících kroků:

1. V modulu snap-in Šablony zabezpečení (Security Templates) vyberte uzel Registry, dlouze ho stiskněte či na něj klepněte pravým tlačítkem myši a poté zvolte příkaz Přidat klíč (Add Key). Tím zobrazíte dialogové okno Vybrat klíč registru (Select Registry Key), znázorněný na obrázku 5–7.



Obrázek 5.7: Vyberte cestu registru či hodnotu, kterou je třeba zabezpečit

2. V dialogovém okně Vybrat klíč registru (Select Registry Key) vyberte cestu k registru nebo hodnotu, se kterou chcete pracovat, a klepněte na tlačítko OK.

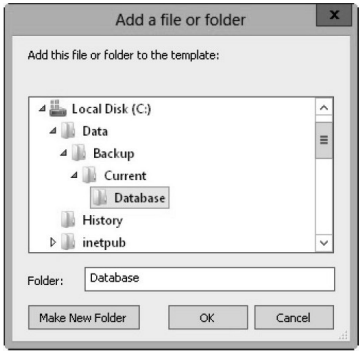
Položky klíče CLASSES_ROOT odpovídají klíči HKEY_CLASSES_ROOT. Položky klíče MACHINE odpovídají klíči HKEY_LOCAL_MACHINE. Položky klíče USERS odpovídají klíči HKEY_USERS.

3. V dialogovém okně Databáze zabezpečení pro (Database Security For) nakonfigurujte požadovaná oprávnění zabezpečení pro uživatele a skupiny. K dispozici máte stejné možnosti pro oprávnění, auditování a vlastnictví jako pro soubory a složky použité se systémem souborů NTFS. Další podrobnosti o oprávnění, auditování a vlastnictví najdete v kapitole 12.
4. Klepněte na tlačítko OK. Zobrazí se dialogové okno Přidat objekt (Add Object). Abyste měli jistotu, že oprávnění pro danou cestu nebo klíč se nenahradí, zvolte možnost Zakázat nahrazení oprávnění k tomuto klíči (Do Not Allow Permissions On This Key To Be Replaced) a poté klepněte na tlačítko OK. Zbývající kroky popisu přeskočte.
5. Pro konfiguraci cesty nebo klíče a nahrazení oprávnění zvolte možnost Nakonfigurovat tento klíč a provést následující akci (Configure This Key Then) a poté zvolte jednu z následujících možností:
   - **Šířit dědičná oprávnění na všechny podklíče (Propagate Inheritable Permissions To All Subkeys)** – tuto možnost zvolte tehdy, chcete-li pro tuto cestu k registru nebo souboru a všechny cesty k registru a souboru pod touto cestou použít všechna oprávnění, která lze zdědit. Existující oprávnění se nahradí pouze tehdy, pokud odporují nastavením oprávnění zabezpečení pro tuto cestu.
   - **Nahradit existují oprávnění ke všem podklíčům dědičnými oprávněními (Replace Existing Permissions On All Subkeys With Inheritable Permissions)** – tuto možnost zvolte pro nahrazení všech existujících oprávnění pro cestu k registru nebo souboru a pro všechny cesty k registru a souboru pod touto cestou. Všechna existující oprávnění se nahradí a zůstanou pouze aktuální oprávnění.
6. Klepněte na tlačítko OK.

Nastavení zabezpečení pro cesty k souboru můžete definovat pomocí následujících kroků:

1. V modulu snap-in Šablony zabezpečení (Security Templates) vyberte uzel File System, dlouze ho stiskněte či na něj klepněte pravým tlačítkem myši a poté zvolte příkaz Přidat soubor (Add File). Tím zobrazíte dialogové okno Přidat soubor nebo složku (Add a File or Folder), znázorněný na obrázku 5.8.
2. V dialogovém okně Přidat soubor nebo složku (Add A File Or Folder) vyberte cestu k souboru nebo složce nebo hodnotu, se kterou chcete pracovat, a klepněte na tlačítko OK.
3. V dialogovém okně Databáze zabezpečení pro (Database Security For) nakonfigurujte požadovaná oprávnění zabezpečení pro uživatele a skupiny. K dispozici

máte stejné možnosti pro oprávnění, auditování a vlastnictví, a to pro soubory a složky použité se systémem souborů NTFS. Další podrobnosti o oprávnění, auditování a vlastnictví najdete v kapitole 12.



Obrázek 5.8: Vyberte cestu k registru nebo hodnotu, kterou chcete zabezpečit

4. Klepněte na tlačítko OK. Zobrazí se dialogové okno Přidat objekt (Add Object). Abyste měli jistotu, že se oprávnění pro danou cestu nenahradí, zvolte možnost Zakázat nahrazení oprávnění k tomuto souboru nebo složce (Do Not Allow Permissions On This File Or Folder) a poté klepněte na tlačítko OK. Zbývající kroky postupu přeskočte.
5. Pro konfiguraci cesty a nahrazení oprávnění zvolte Nakonfigurovat tuto cestu (Configure This Path Then) a poté zvolte jednu z následujících možností:
   - **Šířit dědičná oprávnění na všechny soubory a složky (Propagate Inheritable Permissions To All Subfolders)** – tuto možnost zvolte tehdy, chcete-li pro tuto cestu k souboru a všechny cesty k souboru pod touto cestou použít všechna oprávnění, která lze zdědit. Existující oprávnění se nahradí pouze tehdy, pokud odporují nastavením oprávnění zabezpečení pro tuto cestu.
   - **Nahradit existující oprávnění ke všem souborům a složkám dědičnými oprávněními (Replace Existing Permissions On All Subfolders With Inheritable Permissions)** – tuto možnost zvolte pro nahrazení všech existujících oprávnění pro cestu k souboru a pro všechny cesty k souboru pod touto cestou. Všechna existující oprávnění se nahradí a zůstanou pouze aktuální oprávnění.
6. Klepněte na tlačítko OK.

Analýza, kontrola a použití šablon zabezpečení

Jak už bylo dříve řečeno, modul snap-in Konfigurace a analýza zabezpečení (Security Configuration And Analysis) použijte při aplikaci šablon a porovnání nastavení v šabloně s existujícími nastaveními v počítači. Použitím šablony zajistíte, že počítač bude splňovat specifickou konfiguraci zabezpečení. Porovnání nastavení vám může pomoci

při hledání libovolných rozdílů mezi aktuální implementací a tím, co je definováno v šabloně zabezpečení. To může být rovněž užitečné při zjišťování, zdali se nastavení zabezpečení časem změnila.

Z praxe: Hlavní nevýhodou použití modulu snap-in Konfigurace a analýza zabezpečení (Security Configuration And Analysis) je, že nemůžete nakonfigurovat více počítačů najednou. Můžete nakonfigurovat pouze zabezpečení počítače, na kterém máte spuštěn daný modul snap-in. Pokud tedy chcete tento nástroj použít k provedení konfigurací zabezpečení, musíte se přihlásit a spustit tento nástroj na každém počítači zvlášť. Třebaže u jednotlivých počítačů tento postup funguje, v doméně se nejedná o optimální řešení. V nastavení domény byste měli importovat nastavení šablon zabezpečení do objektu zásad skupiny a tímto způsobem provést konfiguraci zabezpečení u více počítačů. Více informací najdete v části „Použití šablon zabezpečení na více počítačích" dále v této kapitole.

Modul snap-in Konfigurace a analýza zabezpečení (Security Configuration And Analysis) používá k uložení nastavení šablon zabezpečení pracovní databázi a poté aplikuje nastavení z této databáze. Pro analýzu a srovnání jsou nastavení šablon vypsána jako skutečná nastavení databáze a aktuální nastavení počítače jsou vypsána jako skutečná nastavení počítače.

Pamatujte si, že když budete aktivně upravovat šablonu v modulu snap-in Šablony zabezpečení, budete si muset šablonu uložit, aby bylo možno změny analyzovat a použít.

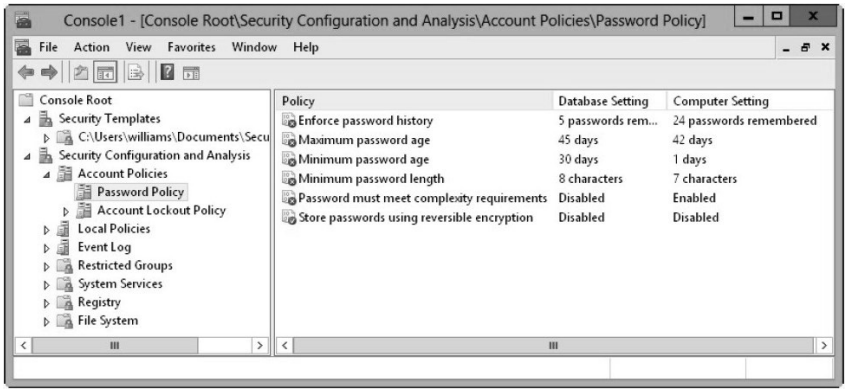
Po vytvoření šablony nebo specifikaci, že chcete použít existující šablonu, můžete nakonfigurovat a analyzovat šablonu pomocí následujících kroků:

1. Otevřete modul snap-in Konfigurace a analýza zabezpečení (Security Configuration And Analysis).
2. Dlouze stiskněte uzel Konfigurace a analýza zabezpečení (Security Configuration And Analysis), či na něj klepněte pravým tlačítkem myši a zvolte příkaz Otevřít databázi (Open Database). Tím zobrazíte dialogové okno Open Database.
3. Standardně je vyhledávací cesta v dialogovém okně Otevřít databázi (Open Database) nastavena na %SystemDrive%\Users\%UserName%\Documents\Security\Database. V případě potřeby najděte pomocí dostupných možností v dialogovém okně Otevřít databázi (Open Database) nové místo uložení. Zadejte popisný název databáze do pole Název souboru (File Name), například **Porovnání aktuální konfigurace**, a poté klepněte na tlačítko Otevřít (Open). Vytvoří se databáze zabezpečení ve formátu Security Database Files s příponou souboru .sdb.
4. Zobrazí se dialogové okno Importovat šablonu (Import Template) s výchozí vyhledávací cestou nastavenou na %SystemDrive%\Users\%UserName%\Documents\Security\Templates. V případě potřeby najděte pomocí dostupných možností v dialogovém okně Importovat šablonu (Import Template) umístění nové

šablony. Vyberte šablonu zabezpečení, kterou chcete použít, a poté klepněte na tlačítko Otevřít (Open). Soubory šablon zabezpečení mají příponu .inf.

5. Dlouze stiskněte uzel Konfigurace a analýza zabezpečení (Security Configuration And Analysis), či na něj klepněte pravým tlačítkem myši na a poté zvolte příkaz Analyzovat počítač (Analyze Computer Now). Po výzvě k nastavení cesty k protokolu událostí zadejte novou cestu nebo použijte výchozí cestu klepnutím na tlačítko OK.
6. Počkejte, až modul snap-in dokončí analýzu vybrané šablony. Pokud během analýzy nastane nějaká chyba, můžete zobrazit protokol chyb dlouhým stisknutím či klepnutím pravým tlačítkem myši na uzel Konfigurace a analýza zabezpečení (Security Configuration And Analysis) a zvolit příkaz Zobrazit soubor protokolu (View Log File).

Pracujete-li s modulem snap-in Konfigurace a analýza zabezpečení (Security Configuration And Analysis), můžete zobrazit rozdíly mezi nastaveními šablony a aktuálním nastavením počítače. Jak znázorňuje obrázek 5.9, nastavení šablony uložená v databázi analýzy, jsou vypsána ve sloupci Nastavení databáze (Database Setting), zatímco aktuální nastavení počítače jsou vypsána ve sloupci Nastavení počítače (Computer Setting). Pokud nebyla nastavení analyzována, je u nich uvedena hodnota Nedefinováno (Not Defined).



Obrázek 5.9: Zkontrolujte si rozdíly mezi nastavením šablony a aktuálním nastavením počítače

Pomocí následujících kroků můžete provádět změny nastavení uložených v databázi:

7. V modulu snap-in Konfigurace a analýza zabezpečení (Security Configuration And Analysis) poklepejte na nastavení, se kterým chcete pracovat.
8. V dialogovém okně Vlastnosti (Properties), které je zobrazeno na obrázku 5.10, si všimněte aktuálního nastavení počítače. Pokud je dostupná informace o účelu nastavení, můžete ji zobrazit klepnutím na kartu Vysvětlit (Explain).