KAPITOLA

9

# Správa registru

Každý, kdo přistupuje k počítači, již někdy pracoval s registrem systému Windows, i když si to možná neuvědomuje. Nezáleží přitom na tom, zda je počítač členem pracovní skupiny nebo domény. Při každém přihlášení jsou z registru načteny uživatelské předvolby. Kdykoli uživatel změní konfiguraci systému, nainstaluje aplikace či hardware nebo jinak změní pracovní prostředí, jsou změny uloženy do registru. Do registru se zaznamenávají i informace o odinstalování hardwaru, aplikací nebo součástí systému.

Registr je centrální úložiště konfiguračních informací v systému Microsoft Windows. Aplikace, součásti systému, ovladače zařízení i jádro operačního systému používají registr k uložení nastavení a načítají z něj údaje o uživatelských předvolbách, konfiguraci systémového hardwaru a výchozích nastaveních systému. Registr také obsahuje data o nastavení zabezpečení, uživatelských právech, místních účtech a mnoho dalších informací. Oproti systému Microsoft Windows NT neukládají novější verze systému Windows do registru informace o účtech domény ani síťových objektech. Tato nastavení spravuje služba AD DS (Active Directory Domain Services), jak je popsáno v části 5, „Správa služby Active Directory a zabezpečení".

Vzhledem k tomu, že registr slouží ke čtení a zápisu značného množství informací, je pro správce zásadně důležité, aby rozuměli jeho struktuře a fungování. Měli byste znát typy dat, se kterými registr pracuje, jaké typy dat se ukládají v jednotlivých částech registru a jak v případě potřeby provést změny. Schopnost měnit registr je důležitá. Když totiž budete chtít vyladit konfiguraci systému nebo opravit chyby, aby se systém choval stabilněji, často je součástí příslušného postupu otevření a úprava registru. Instrukce obvykle předpokládají, že víte, co děláte. Bohužel platí, že pokud se pokusíte provést určitou změnu a přesně nerozumíte jejím principům, může se stát, že systém nepůjde vůbec spustit. Nezapomínejte na to tedy, když se nyní budete seznamovat s tím, jak registr funguje a jak jej lze používat.

**Témata kapitoly**

# Úvod do registru

Registr je uložen jako binární databáze, jejíž informace jsou uspořádány hierarchickou formou. Tato hierarchie má podobnou strukturu jako systém souborů. Jedná se o obrácený strom, který má kořen na svém vrcholu. Pokaždé, kdy musí operační systém Windows získat výchozí systémové hodnoty nebo údaje o uživatelských předvolbách, obrací se na registr. Kdykoli instalujete programy nebo provádíte změny pomocí ovládacích panelů, zpravidla se tyto změny zapisují do registru.

**POZNÁMKA**

Slovo „zpravidla" je v předchozí větě proto, že v doménách systému Windows se některé konfigurační informace zapisují do adresářové služby Active Directory. Počínaje systémem Microsoft Windows 2000 se například pomocí služby Active Directory ukládají údaje o uživatelských účtech a síťových objektech. Když navíc zvýšíte úroveň členského serveru na řadič domény, jsou do služby Active Directory přenesena klíčová nastavení registru, která se týkají serveru, jako např. výchozí konfigurační hodnoty. Tyto hodnoty lze poté spravovat pomocí služby Active Directory. Pokud však později úroveň řadiče domény snížíte, původní nastavení registru tím neobnovíte. Místo toho se obnoví výchozí nastavení, která by byla v platnosti u nově nainstalovaného serveru.

Význam registru spočívá v tom, že ukládá většinu informací o stavu systému. Pokud změníte předvolby a nastavení systému, jsou tyto změny uloženy do registru. Jestliže dojde k selhání systému a nelze jej obnovit, nemusíte instalovat nový systém a poté jej konfigurovat tak, aby vypadal stejně jako původní systém. Místo toho můžete nainstalovat systém Windows Server 2008 a poté obnovit zálohu registru havarovaného systému. Tím do nového systému přenesete všechny předvolby a nastavení starého systému.

Je sice zajímavé, že registr ukládá provedená nastavení, ale možná uvažujete nad tím, jaké jsou jeho další funkce. Kromě ukládání uživatelských nastavení registr uchovává také změny, které provedl operační systém. Jádro operačního systému například do registru ukládá informace, které jsou potřebné pro ovladače zařízení. Patří k nim parametry inicializace ovladačů, díky kterým se ovladače zařízení mohou automaticky konfigurovat tak, aby fungovaly se systémovým hardwarem.

Registr také využívají mnohé další systémové komponenty. Když instalujete systém Windows Server 2008, je na základě možností zvolených při instalaci vytvořena výchozí databáze registru. Instalační program upraví registr pokaždé, kdy přidáte nebo odeberete systémový hardware. Instalační programy aplikací obdobně mění registr, když ukládají příslušná instalační nastavení a zjišťují, které komponenty aplikace jsou již nainstalovány. Spuštěné aplikace pak znovu využívají nastavení registru.

Na rozdíl od předchozích verzí systému Windows však systémy Windows Vista a Windows Server 2008 pokaždé neukládají nastavení aplikací přímo do registru a ve skutečnosti mohou načítat některá nastavení z uživatelského profilu. Toto nové chování se objevuje kvůli nástroji Řízení uživatelských účtů (User Account Control – UAC). Nástroj Řízení uživatelských účtů kromě mnoha dalších vlastností implementuje dvě klíčové funkce, které mění způsob, jakým systém Windows instaluje a spouští aplikace: úrovně spuštění aplikací a virtualizaci aplikací.

Kvůli kompatibilitě s úrovněmi spuštění a virtualizací jsou všechny aplikace, které jsou spuštěny v systémech Windows Vista a Windows Server 2008, vybaveny tokenem zabezpečení. Token zabezpečení odráží úroveň oprávnění, která jsou požadována ke spuštění aplikace. Aplikace

vytvořené pro systémy Windows Vista a Windows Server 2008 mohou mít token *správce* nebo token *standardního uživatele*. Aplikace s tokeny správce vyžadují ke svému spuštění a provádění základních úkolů vyšší oprávnění. Když je aplikace s tokenem správce spuštěna v režimu s vyššími oprávněními, může vykonávat úkoly, které vyžadují oprávnění správce. Kromě toho smí zapisovat do systémových umístění v registru a systému souborů.

Aplikace s tokeny standardního uživatele na druhou stranu ke spuštění a plnění klíčových funkcí nevyžadují vyšší oprávnění. Jakmile je aplikace s tokenem standardního uživatele spuštěna ve standardním uživatelském režimu, musí při provádění úkolů správy požádat o vyšší oprávnění. V případě všech ostatních úloh by aplikace neměla fungovat s vyššími oprávněními. Aplikace by dále měly zapisovat data pouze do nesystémových oblastí registru a systému souborů.

Standardní uživatelské aplikace jsou spuštěny ve speciálním režimu kompatibility a zobrazují virtuální prostředky pomocí virtualizace systému souborů a registru. Když se aplikace pokusí zapsat do systémového umístění, poskytne systém Windows Vista nebo Windows Server 2008 aplikaci soukromou kopii souboru nebo hodnoty registru. Všechny změny jsou poté zapsány do soukromé kopie, která je následně uložena v datech uživatelského profilu. Pokud se aplikace pokusí znovu zapisovat nebo číst toto systémové umístění, dostane od systému soukromou kopii z uživatelského profilu, kterou může používat. Jestliže dojde k chybě při zpracování virtualizovaných dat, vztahují se ve výchozím nastavení oznámení o chybách a informace protokolu k virtualizovanému umístění, nikoli ke skutečnému umístění, se kterým se aplikace pokoušela pracovat.



**DO DETAILU**

**Transakční registr**

Systém Windows Server 2008 implementuje ve svém jádře transakční technologii, která při zápisu do systému souborů NTFS a registru zachovává integritu dat a obsluhuje chybové stavy. Aplikace naprogramované tak, aby využívaly transakčního registru, mohou spravovat změny registru pomocí transakcí jako diskrétní operace, které lze v případě úspěchu potvrdit nebo v případě neúspěchu vrátit. Zatímco je transakce aktivní, nejsou změny registru pro uživatele ani jiné aplikace viditelné. Teprve když systém Windows Server 2008 transakci potvrdí, jsou změny plně aplikovány a lze je sledovat. Transakce použité s registrem lze koordinovat s libovolným jiným transakčním prostředkem, jako je služba MSMQ (Microsoft Message Queuing). Pokud dojde při zpracování transakce k chybě operačního systému, jsou potvrzené operace zapsány na disk a nedokončené transakční operace jsou vráceny.

**DO DETAILU**

**Řízení virtualizace**

Virtualizaci registru lze povolit nebo zakázat v Místních zásadách zabezpečení (Local Security Policy), v sekci Možnosti zabezpečení (Security Options). V systémech Windows Vista a Windows Server 2008 je pro tento účel k dispozici nové nastavení zabezpečení: Řízení uživatelských účtů: (User Account Control:) Virtualizovat chyby zápisu do souboru a registru do umístění jednotlivých uživatelů (Virtualize File and Registry Write Failures to Per-User Locations). Toto nastavení zabezpečení umožňuje přesměrovat chyby zápisu starších aplikací do definovaných umístění v registru a systému souborů. Tato funkce umožňuje používat starší programy, které ke svému spuštění vyžadují oprávnění správce. Toto nastavení, které je standardně povoleno, umožňuje přesměrovat chyby zápisu aplikací do definovaných uživatelských umístění jak v systému souborů, tak v registru. Když toto nastavení zakážete, budou aplikace, které zapisují data do chráněných umístění, ukončeny bez oznámení chyby.

Chcete-li zobrazit nebo upravit toto nastavení v konzole Místní nastavení zabezpečení (Local Security Settings), klepněte na tlačítko Start, příkaz Nástroje pro správu (Administrative Tools) a poté na položku Místní zásady zabezpečení (Local Security Policy). Zobrazí se konzola Místní zásady zabezpečení (Local Security Policy). V levém podokně rozbalte uzel Místní zásady (Local Policies) a vyberte uzel Možnosti zabezpečení (Security Options). V hlavním podokně by se měl zobrazit seznam nastavení zásad. Pomocí posuvníku přejděte v seznamu dolů na nastavení zabezpečení. Poklepejte na zásadu Řízení uživatelských účtů: (User Account Control:) Virtualizovat chyby zápisu do souboru a registru do umístění jednotlivých uživatelů (Virtualize File and Registry Write Failures to Per-User Locations). Na kartě Místní nastavení zabezpečení (Local Policy Setting) dialogového okna se zobrazí aktuální stav zásady (povoleno nebo zakázáno). Chcete-li změnit stav nastavení, klepněte podle potřeby na přepínač Povolit (Enabled) nebo Zakázat (Disabled) a poté klepněte na tlačítko OK.

# Seznámení se strukturou registru

Mnohé nástroje pro správu ve skutečnosti poskytují pouze snadno použitelné uživatelské rozhraní pro práci s registrem. Zejména to platí pro ovládací panely. Nemusíte tedy manipulovat přímo s určitou oblastí registru, ale můžete využít nástroje společnosti Microsoft, díky nimž lze potřebné změny provést bezpečně a spolehlivě. Používejte tyto nástroje – jsou zde pro vás.

**UPOZORNĚNÍ**

Nelze dostatečně zdůraznit, jak důležité je měnit registr pomocí správných nástrojů. Pokud lze určitou oblast registru měnit pomocí specializovaného nástroje, měli byste jej používat. Nevrtejte se v registru jen proto, že vám v tom nic nebrání. Pokud registr změníte nesprávným způsobem, můžete ohrozit stabilitu systému a v některých případech dokonce znemožnit jeho spuštění.

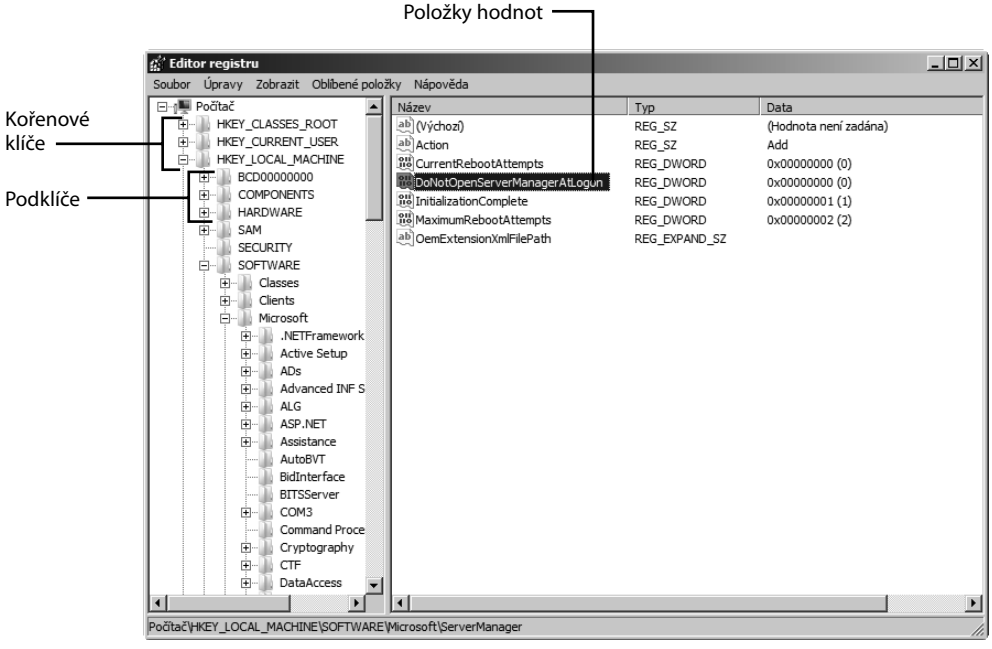
Jak vidíte, téměř všechny činnosti v operačním systému nějakým způsobem ovlivňují registr. Proto je tak důležité rozumět, k čemu se registr používá, jak s ním lze pracovat, jak jej zabezpečit a jakým způsobem jej můžete spravovat.

Registr je v prvé řadě databáze. Podobně jako libovolná jiná databáze je také registr určen k ukládání a načítání informací. Libovolnou hodnotu registru lze identifikovat zadáním cesty k příslušnému umístění. Například cesta HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon označuje hodnotu registru, pomocí níž můžete povolit nebo zakázat automatické zobrazení Správce serveru při přihlášení.

Tato hodnota registru je znázorněna na obrázku 9.1. Vzhledem ke své hierarchické struktuře je registr zdánlivě uspořádán podobně jako systém souborů. Jeho strukturu lze skutečně přirovnat k systému souborů. Tato analogie je však poněkud zavádějící, protože na pevném disku systému nenajdete žádné skutečné složky a soubory, které by odpovídaly struktuře registru. Vlastní fyzická struktura registru nezávisí na tom, jak jsou data registru reprezentována. Umístění v registru jsou zastoupena logickou strukturou, která jen volně souvisí s tím, jak jsou uloženy položky hodnot.

Na rozdíl od systémů Windows 2000 a Windows NT podporují systémy Windows Server 2003 a Windows Server 2008 registry větší velikosti než dříve. Již také neudržují celý registr ve stránkovaném fondu paměti. Místo toho jsou podle potřeby do systémové mezipaměti mapovány

pohledy registru s velikostí 256 kilobajtů (kB). Jedná se o důležitou změnu původní architektury registru, která v zásadě omezovala velikost registru asi na 80 procent celkové velikosti stránkovaného fondu paměti. Nová implementace registru je omezena pouze dostupným místem ve stránkovacím souboru.




**Obrázek 9.1:** Přístup k hodnotě podle její cesty v registru

Při spuštění systému jsou do systémové paměti mapovány pohledy registru s velikostí 256 kB. Díky tomu může systém Windows Server 2008 rychle načíst informace o konfiguraci. Některé údaje registru se vytvářejí dynamicky na základě hardwarové konfigurace při spuštění systému a existují teprve poté, kdy jsou sestaveny. Převážná část registru se však ukládá v trvalé formě na disk a příslušná data se načítají ze sady souborů, které se označují jako podregistry (hive). *Podregistry* jsou binární soubory, které reprezentují seskupení klíčů a hodnot. Soubory podregistru naleznete v adresáři %SystemRoot%\System32\Config. V tomto adresáři se nacházejí také soubory .sav a .log, které slouží jako záložní soubory registru.

**DO DETAILU**

**Systém Windows Server 2008 spravuje velikost registru a spotřebu paměti**

Systémy Windows NT a Windows 2000 ukládají celý registr do stránkovaného fondu paměti. U 32bitových systémů z toho vyplývá omezení registru přibližně na 160 megabajtů (MB), což je dáno rozložením virtuálního adresního prostoru v jádru operačního systému. Když se v této konfiguraci registr rozrůstá, bohužel spotřebovává značnou část stránkovaného fondu paměti. Přitom může zůstat příliš málo paměti pro jiné komponenty režimu jádra.

Systémy Windows Server 2003 a Windows Server 2008 tento problém řeší tak, že mění způsob uložení registru do paměti. V rámci nové implementace načítá správce mezipaměti (Cache Manager) do systémové mezipaměti podle potřeby mapované pohledy registru s velikostí 256 kB. Zbytek registru je uložen do stránkovacího souboru na disku. Vzhledem k tomu, že se registr zapisuje do systémové mezipaměti, může být umístěn v systémové paměti RAM (Random Access Memory) a systém jej může podle potřeby přesunovat mezi pamětí a stránkovacím souborem. Předchozí verze operačního systému Windows umožňovaly nastavit maximální velikost paměti a místa na disku, které mohl registr obsadit. Díky zlepšeným funkcím správy paměti nyní spotřebu paměti registrem automaticky nastavuje operační systém. Většina členských serverů používá pro registr mezi 20 a 25 MB paměti. Řadiče domény nebo servery s mnoha součástmi konfigurace, službami a aplikacemi mohou paměti spotřebovat mnohem více. Jednomu z klíčových řadičů domény v naší organizaci však pro registr postačuje jen 25 až 30 MB paměti. Z toho je zřejmé, že došlo ke značným změnám oproti starší architektuře, kde mohly paměťové požadavky registru vzrůst až na 160 MB.

Ke čtení registru potřebujete speciální editor. Editor, který je k dispozici v systému Windows Server 2008, se nazývá Editor registru (Registry Editor). Pomocí Editoru registru můžete procházet logickou strukturu registru od vrcholu databáze až na nejnižší úroveň. Shora dolů se úrovně databáze označují jako kořenové klíče, podklíče a položky hodnot.

**DO DETAILU**

**Regedit nahrazuje Regedt32**

Oproti předchozím verzím operačního systému Windows, které obsahovaly dvě verze Editoru registru, se systémy Windows Server 2003 a Windows Server 2008 dodávají s jedinou verzí. Tato verze s názvem Regedit.exe integruje všechny funkce obou původních editorů registru. Z originálního programu Regedit.exe přebírá klíčové funkce. Z programu Regedt32.exe, který již nadále není k dispozici, získává funkce zabezpečení a oblíbených položek. Pomocí funkce Oprávnění (Permissions) můžete zobrazovat a spravovat oprávnění k hodnotám registru. Funkce Oblíbené položky (Favorites) dovoluje vytvářet a používat oblíbené položky, které poskytují rychlý přístup k uloženým umístěním v rámci registru.

Program Regedt32 ***opravdu*** zmizel – ačkoli se na něj stejně jako mnoho jiných správců stále odkazuji. Nakonec se jedná o editor, který správci používali, protože umožňoval spravovat zabezpečení registru. Tento nástroj se správcům také doporučoval místo programu Regedit. Zvyk je železná košile a systém Windows Server 2008 proto stále obsahuje zástupný soubor Regedt32. Pokud však program Regedt32 spustíte, operační systém ve skutečnosti spustí nástroj Regedit.

Na vrcholu hierarchie registru se nacházejí kořenové klíče. Každý kořenový klíč obsahuje několik podklíčů, které sdružují další podklíče a položky hodnot. Názvy položek hodnot musí být v rámci příslušného podklíče jedinečné a položky hodnot odpovídají konkrétním parametrům konfigurace. Nastavení těchto parametrů konfigurace je určeno hodnotami, které jsou uloženy v dané položce hodnoty. Každá hodnota má přidružen datový typ, který rozhoduje o typu dat, jaká lze do položky uložit. Některé položky hodnot se například používají pouze k uložení binárních dat, zatímco jiné uchovávají pouze řetězce znaků. Tyto rozdíly závisejí na datovém typu hodnoty.

Nyní můžeme rozdělit cestu registru HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AllowMultipleTSSessions tak, aby byla srozumitel-

nější. Kořenovým klíčem je zde *HKEY_LOCAL_MACHINE*. Každá položka mezi kořenovým klíčem a údajem *AllowMultipleTSSessions* představuje úroveň podklíče v hierarchii registru. Nakonec *AllowMultipleTSSessions* je vlastní položka hodnoty.

Registr je velmi složitý a často vypadá ještě nepřehledněji, protože se v příslušné dokumentaci používají různé termíny nad rámec těch, které jsme již zmínili. Když budete číst různé informační zdroje o registru, můžete se setkat s následujícími odkazy:

- **Podstromy** – *podstrom* (subtree) je název stromu klíčů a hodnot, který vychází z kořenového klíče a postupuje k nižším úrovním hierarchie registru. V dokumentaci se kořenové klíče často označují jako podstromy. Když autoři dokumentace zmiňují podstrom, mají tím na mysli větev klíčů a hodnot, která je obsažena v rámci uvedeného kořenového klíče.
- **Klíče** – kořenové klíče jsou technicky vrcholem hierarchie registru. Pod kořenovým klíčem se pak nacházejí výhradně podklíče nebo položky hodnot. Podklíče se však v praxi označují termínem klíče. Je prostě snazší popisovat určitou položku jako klíč. Lze to přirovnat k tomu, kdy při popisu cesty v systému souborů říkáme „ta a ta složka" namísto „podsložka".
- **Hodnoty** – *hodnota* (value) je nejnižší úroveň hierarchie registru. Pro zjednodušení se položky hodnot často jednoduše označují jako hodnoty. Technicky však položka hodnoty zahrnuje tři části: název, datový typ a hodnotu. Název identifikuje nastavení konfigurace. Datový typ identifikuje formát dat. Hodnota obsahuje skutečná data v rámci položky.



Když jste nyní obeznámeni se základy struktury registru, můžete se pustit dále a podívat se podrobněji na kořenové klíče, hlavní podklíče a datové typy.

# Kořenové klíče registru

Registr je uspořádán do hierarchie klíčů, podklíčů a položek hodnot. Kořenové klíče jsou umístěny na nejvyšší úrovni hierarchie a tvoří primární větve neboli podstromy údajů registru. Registr obsahuje dva fyzické kořenové klíče: HKEY_LOCAL_MACHINE a HKEY_USERS. Tyto fyzické kořenové klíče souvisejí s konkrétními soubory uloženými na disku. Dělí se na další logické skupiny informací registru. Jak je patrné v tabulce 9.1, logické skupiny jsou jednoduše podmnožiny informací, které jsou shromážděny v klíčích HKEY_LOCAL_MACHINE a HKEY_USERS.

**Tabulka 9.1:** Podstromy registru

| Podstrom | Popis |
|---|---|
| **Fyzický podstrom** | |
| HKEY_LOCAL_MACHINE (HKLM) | Ukládá všechna nastavení, která se týkají hardwaru aktuálně nainstalovaného v počítači. |
| HKEY_USERS (HKU) | Ukládá data uživatelských profilů pro všechny uživatele, kteří se dosud k počítači místně přihlásili, a také výchozí uživatelský profil. |

| Podstrom | Popis |
|---|---|
| **Logický podstrom** | |
| HKEY_CLASSES_ROOT (HKCR) | Ukládá všechna přidružení souborů a identifikátory tříd propojování a vkládání objektů (OLE). Tento podstrom je vytvořen z klíčů HKEY_LOCAL_MACHINE\SOFTWARE\Classes a HKEY_CURRENT_USER\SOFTWARE\Classes. |
| HKEY_CURRENT_CONFIG (HKCC) | Ukládá informace o hardwarové konfiguraci při spuštění systému. Tento podstrom je vytvořen z klíče HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current, který sám o sobě odkazuje na číslovaný podklíč s aktuálním profilem hardwaru. |
| HKEY_CURRENT_USER (HKCU) | Ukládá informace o aktuálně přihlášeném uživateli. Tento klíč obsahuje ukazatel na klíč HKEY_USERS\UserSID, kde UserSID je identifikátor zabezpečení aktuálního uživatele a také dříve popsaného výchozího profilu. |

**DO DETAILU**

**Registr v 64bitových systémech Windows**

Registr v 64bitových systémech Windows se dělí na 32bitové a 64bitové klíče. Mnoho klíčů je vytvořeno jak ve 32bitové, tak v 64bitové verzi, a i když tyto klíče patří do jiných větví registru, mají stejný název. Editor registru (Regedit.exe) je v těchto systémech navržen tak, aby pracoval s 32bitovými i 64bitovými klíči. 32bitové klíče jsou však reprezentovány přesměrovačem registru WOW64 a zobrazují se pod klíčem HKEY LOCAL MACHINE\SOFTWARE\WOW6432Node. Chcete-li s 32bitovými klíči pracovat přímo, můžete k tomu použít 32bitový editor registru, který naleznete v umístění %SystemRoot%\Syswow64\Regedit.

Kvůli podpoře spolupráce 32bitových a 64bitových komponent v modelu COM (Component Object Model) a používání 32bitových programů zrcadlí přesměrovač WOW64 klíče a hodnoty registru související s modelem COM mezi 64bitovými a 32bitovými zobrazeními registru. Klíče a hodnoty jsou někdy v procesu reflexe upraveny, aby se přizpůsobily názvy cest a jiné hodnoty, které mohou záviset na verzi. To v důsledku znamená, že se 32bitové a 64bitové hodnoty mohou lišit.

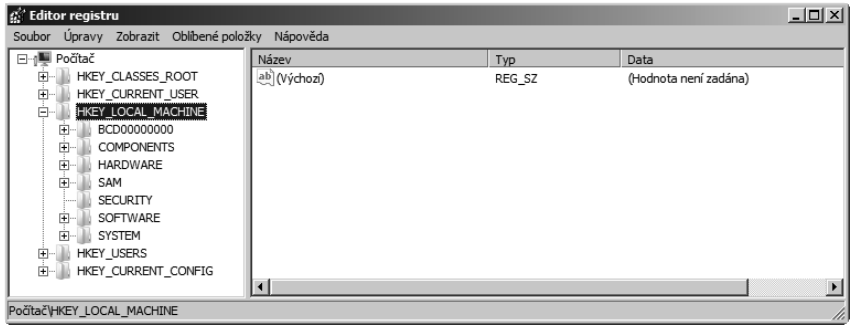
## HKEY_LOCAL_MACHINE

Klíč HKEY_LOCAL_MACHINE (zkráceně HKLM) obsahuje všechna nastavení, která se týkají hardwaru aktuálně nainstalovaného v systému. Zahrnuje nastavení paměti, ovladačů zařízení, nainstalovaného hardwaru a spouštění systému. Aplikace by měly ukládat nastavení do klíče HKLM pouze v případě, že se příslušná data týkají všech uživatelů počítače.

Jak je vidět na obrázku 9.2, obsahuje klíč HKLM následující hlavní podklíče:

- COMPONENTS
- HARDWARE
- SAM
- SECURITY
- SOFTWARE
- SYSTEM

Tyto podklíče si rozebereme v následujících oddílech.




**Obrázek 9.2:** Přístup ke klíči HKEY_LOCAL_MACHINE registru



### HKLM\COMPONENTS

Systémy Windows Vista a Windows Server 2008 ukládají informace o aktualizacích a funkcích systému Windows do datového úložiště. Tyto operační systémy používají klíč HKLM\COMPONENTS k uchování informací, které se týkají konfigurace a stavu datového úložiště. K těmto údajům patří architektura úložiště a verze formátu. Systémy Windows Vista a Windows Server 2008 mění toto datové úložiště při každém stažení nebo nainstalování aktualizací a také v případě přidání či odebrání funkcí.

**POZNÁMKA**

Pokud je datové úložiště komponent poškozeno, může se zobrazit kód chyby 0x80073712 pokaždé, kdy se pokusíte instalovat aktualizaci z webu služby Windows Update. V některých případech se také nezobrazují funkce systému Windows, chcete-li je přidat nebo odebrat. V tomto případě můžete systému Windows sdělit, že úložiště bylo poškozeno, a je tedy nutné je obnovit. Na příkazový řádek se zvýšenými oprávněními zadejte následující příkaz: **reg delete HKLM\COMPONENTS /v StoreDirty**. Další informace naleznete v článku znalostní báze Microsoft Knowledge Base 931712 (***http://support.microsoft.com/kb/931712***).

### HKLM\HARDWARE

Klíč HKLM\HARDWARE ukládá informace o konfiguraci hardwaru počítače. Operační systém Windows Server 2008 tento klíč znovu vytvoří při každém spuštění. Klíč se nachází pouze v paměti, nikoli na disku. Při vytváření klíče operační systém vytvoří výčet všech zařízení, která lze zjistit. Systém prohledá systémové sběrnice a pokusí se zjistit zařízení z konkrétních tříd, jako jsou sériové porty, klávesnice a polohovací zařízení.

V rámci klíče HKLM\HARDWARE naleznete standardní podklíče, které se dynamicky vytvářejí při spuštění a obsahují informace získané operačním systémem. Jedná se o následující podklíče:

- **ACPI** – obsahuje informace o rozhraní ACPI (Advanced Configuration Power Interface), což je součást systému BIOS, která podporuje technologii plug-and-play a pokročilé funkce řízení spotřeby. V počítačích, které nejsou kompatibilní se standardem ACPI, tento podklíč neexistuje.

- **DESCRIPTION** – obsahuje popis hardwaru, včetně hardwarových zařízení hlavního procesoru počítače, matematického koprocesoru a multifunkčních adaptérů. U přenosných počítačů uvádí jedno z multifunkčních zařízení informace o stavu dokování. V případě počítačů s víceúčelovými čipovými sadami poskytuje jedno z multifunkčních zařízení údaje o řadičích disků, klávesnic, paralelních portů, sériových portů a polohovacích zařízení. K dispozici je také univerzální kategorie pro další řadiče, která se využívá například tehdy, pokud počítač obsahuje řadič karet PC Card.
- **DEVICEMAP** – obsahuje informace, které mapují zařízení na ovladače zařízení. Najdete zde mapování zařízení pro klávesnice, ukazovací zařízení, paralelní porty, porty SCSI (Small Computer System Interface), sériové porty a videozařízení. Za pozornost stojí zejména fakt, že podklíč VIDEO obsahuje položku hodnoty pro grafické zařízení kompatibilní se standardem VGA, které je v počítači nainstalováno. Toto zařízení se použije v případě, že je nutné spustit počítač v režimu zobrazení VGA.
- **RESOURCEMAP** – obsahuje mapování vrstvy HAL (Hardware Abstraction Layer), správce plug-and-play a dostupných systémových prostředků. Všimněte si hlavně správce plug-and-play (Plug and Play Manager). Do tohoto podklíče zaznamenává údaje o zařízeních, která umí obsluhovat.

Další nestandardní podklíče se mohou vyskytovat v sekci HKLM\HARDWARE. Podklíče jsou specifické pro hardware počítače.

### HKLM\SAM

Klíč HKLM\SAM uchovává databázi správce účtů zabezpečení (Security Accounts Manager – SAM). Vytvoříte-li ve členských serverech a pracovních stanicích místní uživatele a skupiny, jsou účty uloženy v klíči HKLM\SAM, stejně jako dříve v systému Windows NT. Tento klíč také obsahuje informace o předdefinovaných uživatelských účtech a účtech skupin a také o členství ve skupinách a aliasech účtů.

Údaje umístěné v klíči HKLM\SAM nejsou ve výchozím nastavení přístupné pomocí Editoru registru. Jedná se o bezpečnostní funkci, která chrání zabezpečení a integritu systému.

### HKLM\SECURITY

Klíč HKLM\SECURITY ukládá informace o místním počítači. Obsahuje data o přihlašovacích pověřeních v mezipaměti, nastaveních zásad, nastaveních zabezpečení souvisejících se službami a výchozích hodnotách zabezpečení. Zahrnuje také kopii klíče HKLM\SAM. Stejně jako u podklíče HKLM\SAM platí, že tento podklíč není přístupný z Editoru registru. Jedná se o bezpečnostní funkci, která chrání zabezpečení a integritu systému.

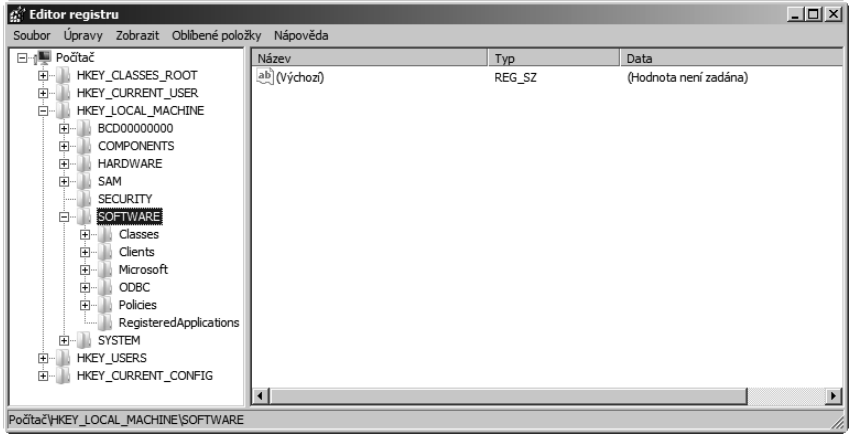
### HKLM\SOFTWARE

Klíč HKLM\SOFTWARE ukládá globální nastavení všech aplikací a komponent nainstalovaných v systému. Jedná se mj. o instalační informace, cesty ke spustitelným souborům, výchozí nastavení konfigurace a registrační informace. Vzhledem k tomu, že se tento podklíč nachází pod klíčem HKLM, jsou informace uložené na tomto místě platné pro celý systém. V tom spočívá rozdíl oproti nastavením konfigurace v klíči HKCU\SOFTWARE, která se aplikují pro jednotlivé uživatele.

Jak je patrné na obrázku 9.3, v klíči HKLM\SOFTWARE najdete mnoho důležitých podklíčů včetně následujících:

- **Classes** – obsahuje všechna přidružení souborů a identifikátory tříd OLE. Jedná se zároveň o klíč, ze kterého se odvozuje klíč HKEY_CLASSES_ROOT.
- **Clients** – ukládá informace o protokolech a prostředích, které používají všechny klientské aplikace nainstalované v systému. Patří sem klienti kalendáře, kontaktů, e-mailů, médií a zpráv.
- **Microsoft** – obsahuje informace o všech aplikacích a komponentách společnosti Microsoft, které jsou v systému nainstalovány. Klíč zahrnuje kompletní nastavení konfigurace, výchozí hodnoty, registrační informace a mnoho dalších dat. Většinu předvoleb grafického uživatelského rozhraní (GUI) naleznete v podklíči HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion. Nastavení konfigurace většiny součástí systému, jazykových sad, oprav Hotfix a dalších komponent je uloženo v podklíči HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion.
- **ODBC** – obsahuje informace o konfiguraci ODBC (Open Database Connectivity) v systému. Zahrnuje údaje o všech ovladačích ODBC a názvech zdrojů dat ODBC (DSN).
- **Policies** – obsahuje informace o místních zásadách pro aplikace a komponenty nainstalované v systému.





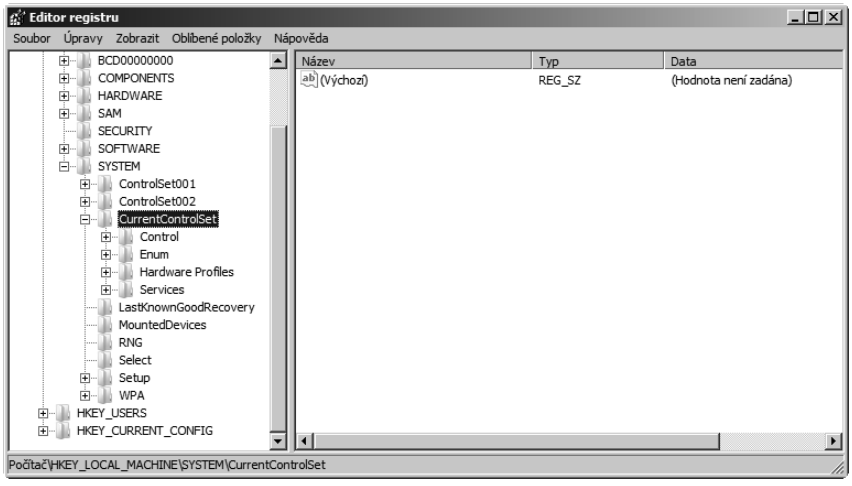

**Obrázek 9.3:** Přístup ke klíči HKEY_LOCAL_MACHINE\SOFTWARE v registru

### HKLM\SYSTEM

Klíč HKLM\SYSTEM ukládá informace o ovladačích zařízení, službách, parametrech spouštění a o dalších nastaveních platných pro celý počítač. V rámci klíče HKLM\SYSTEM se nachází několik důležitých podklíčů. Mezi nejvýznamnější patří podklíč HKLM\SYSTEM\CurrentControlSet (viz obrázek 9.4).

Podklíč CurrentControlSet obsahuje informace o sadě ovládacích prvků a služeb, jež se používají od posledního úspěšného spuštění systému. Tento podklíč vždy shrnuje údaje o sadě ovládacích prvků, které jsou aktuálně aktivní, a reprezentuje poslední úspěšné spuštění. Operační systém zapisuje sadu ovládacích prvků v posledním kroku procesu spouštění. Registr je tedy aktualizován tak, aby odrážel sadu ovládacích prvků a služeb použitých při nejaktuálnějším úspěšném spuštění. Tato data v praxi umožňují spustit systém v poslední

známé funkční konfiguraci (Last Known Good Configuration), když systém havaruje nebo dojde k chybě Stop.




**Obrázek 9.4:** Přístup k podklíči HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet v registru

Klíč HKLM\SYSTEM také zahrnuje dříve vytvořené sady ovládacích prvků. Tyto sady jsou uloženy v podklíčích s názvy ControlSet001, ControlSet002 atd. V rámci sad ovládacích prvků naleznete čtyři důležité podklíče:

- **Control** – obsahuje řídicí informace o klíčových nastaveních operačního systému, nástrojích a dílčích komponentách, včetně vrstvy HAL, rozloženích klávesnice, systémových zařízeních, rozhraních a třídách zařízení. V rámci podklíče BackupRestore se nacházejí uložená nastavení nástroje Zálohování, která zahrnují seznamy klíčů nástroje Automatické obnovení systému (Automated System Recovery – ASR), souborů a nastavení registru, které nebudou obnoveny. V podklíči SafeBoot jsou umístěny sady ovládacích prvků, které slouží pro minimální spuštění systému a spuštění pouze s podporou sítě.
- **Enum** – obsahuje kompletní výčet zařízení nalezených v počítači, když operační systém vyhledal konkrétní třídy zařízení na systémových sběrnicích. Jedná se o úplný seznam zařízení, která byla přítomna při spuštění operačního systému.
- **Hardware Profiles** – obsahuje podklíč pro každý profil hardwaru dostupný v systému. První profil hardwaru označený kódem 0000 je prázdný. Další očíslované profily počínaje kódem 0001 reprezentují profily, které jsou v systému k dispozici. Profil označený Current vždy odkazuje na profil, který se v operačním systému aktuálně používá.
- **Services** – obsahuje podklíč pro každou službu nainstalovanou v systému. Tyto podklíče uchovávají potřebné konfigurační informace pro související služby, které mohou zahrnovat spouštěcí parametry a také nastavení zabezpečení a výkonu.

Dalším zajímavým podklíčem je HKLM\SYSTEM\MountedDevices. Operační systém vytváří tento klíč a ukládá do něj seznam připojených a dostupných diskových zařízení. Disková zařízení jsou uvedena podle konfigurace logických svazků a přiděleného písmene jednotky.

## HKEY_USERS

Klíč HKEY_USERS (zkráceně HKU) obsahuje data uživatelských profilů všech uživatelů, kteří se dosud k počítači místně přihlásili, a také výchozí uživatelský profil. Vlastníkem každého uživatelského profilu je příslušný uživatel, pokud nezměníte oprávnění nebo profily nepřesunete. K nastavením profilu patří konfigurace plochy uživatele, proměnné prostředí, možnosti složky, možnosti nabídek, tiskárny a síťová připojení.

Uživatelské profily se ukládají do podklíčů klíče HKEY_USERS podle svých identifikátorů zabezpečení (SID). Naleznete zde také podklíč *IDzabezpečení*_Classes, který reprezentuje přidružení souborů, která se týkají daného uživatele. Pokud například uživatel nastaví Adobe Photoshop jako výchozí program pro práci se soubory .jpeg a .jpg a toto nastavení se liší od výchozích hodnot systému, budou v tomto podklíči umístěny položky s příslušným přidružením souborů.

Používáte-li zásady skupin (viz část 5), aplikují se nastavení zásad na jednotlivé uživatelské profily uložené v tomto klíči. Výchozí profil určuje, jak se počítač chová v případě, že není přihlášen žádný uživatel. Slouží také jako základní profil pro nové uživatele přihlášené k počítači. Jestliže například chcete zajistit, že nebude-li přihlášen žádný uživatel, použije systém spořič obrazovky chráněný heslem, můžete příslušným způsobem upravit výchozí profil. Podklíč výchozího uživatelského profilu lze snadno rozpoznat, protože je označen HKEY_USERS\.DEFAULT.

**POZNÁMKA**

Informace profilu umístěné v klíči HKU jsou načteny z dat profilu, která jsou uložena na disku. Výchozí umístění profilů je %SystemDrive%\Users***UživatelskéJméno***, kde ***UživatelskéJméno*** je přihlašovací jméno uživatele kompatibilní se staršími systémy než Windows 2000.

## HKEY_CLASSES_ROOT

Klíč HKEY_CLASSES_ROOT, který se zkráceně označuje jako HKCR, ukládá všechna přidružení souborů. Tato přidružení obsahují informace o tom, které typy souborů dokumentů jsou přidruženy k jednotlivým aplikacím, a také o tom, jakou akci má systém provést v případě různých úkolů s konkrétním typem dokumentu, např. při otevření, úpravách, zavření nebo přehrání. Pokud například poklepete na soubor typu .doc, obvykle se dokument otevře pro úpravy v aplikaci Microsoft Word. Toto přidružení souboru je doplněno do klíče HKCR při instalaci sady Microsoft Office nebo aplikace Microsoft Word. Jestliže není nainstalována sada Microsoft Office ani program Microsoft Word, je soubor s příponou .doc místo toho otevřen v programu WordPad. Jedná se totiž o výchozí přidružení souboru vytvořené po instalaci operačního systému.

Klíč HKCR je založen na klíčích HKEY_LOCAL_MACHINE\SOFTWARE\Classes a HKEY_CURRENT_USER\SOFTWARE\Classes. První uvedený klíč poskytuje registrace tříd specifické pro počítač a druhý z obou klíčů dodává registrace tříd pro konkrétního uživatele. Vzhledem k tomu, že uživatelsky specifické registrace tříd mají přednost, může mít každý uživatel počítače zaregistrovány odlišné třídy. Jedná se o rozdíl oproti předchozím verzím operačního systému Windows, kde měli všichni uživatelé konkrétního počítače k dispozici stejné informace o registraci tříd.

### HKEY_CURRENT_CONFIG

Klíč HKEY_CURRENT_CONFIG (zkráceně HKCC) obsahuje informace o hardwarové konfiguraci při spuštění systému, která se také označuje jako spouštěcí konfigurace počítače. Tento klíč zahrnuje údaje o aktuálním přiřazení zařízení, ovladačích zařízení a systémových službách, které byly k dispozici při spuštění.

Klíč HKCC se vytváří z klíče HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Hardware Profiles\Current, který sám o sobě odkazuje na číslovaný podklíč s aktuálním profilem hardwaru. Má-li systém více profilů hardwaru, směřuje klíč na odlišný profil hardwaru v závislosti na stavu spouštění nebo na profilu hardwaru vybraném při spuštění.

### HKEY_CURRENT_USER

Klíč HKEY_CURRENT_USER (zkráceně HKCU) obsahuje informace o aktuálně přihlášeném uživateli. Tento klíč obsahuje ukazatel na klíč HKEY_USERS*UserSID*, kde *UserSID* je identifikátor zabezpečení aktuálního uživatele a také dříve popsaného výchozího profilu. Společnost Microsoft požaduje, aby aplikace ukládaly uživatelsky specifické předvolby do tohoto klíče. V tomto klíči jsou například uložena nastavení jednotlivých uživatelů sady Microsoft Office. Jak jsme již uvedli, obsahuje podklíč HKEY_CURRENT_USER\SOFTWARE\Classes také uživatelsky specifická nastavení pro přidružení souborů.

**POZNÁMKA**

Pokud nechcete, aby uživatelé mohli nastavovat své vlastní přidružení souborů, můžete změnit oprávnění k podklíči HKLM\SOFTWARE\Classes. Uživatelé pak nebudou moci upravit globální nastavení, která jim chcete přidělit. Další informace o oprávněních registru naleznete v oddíle „Zabezpečení registru" na straně 287.

## Data registru: jak se ukládají a používají

Když nyní lépe rozumíte struktuře registru, podívejme se na to, jaká data vlastně registr obsahuje. Znalost toho, jak se data registru ukládají a používají, je stejně důležitá jako znalost samotné struktury registru.

### Původ dat registru

Jak jsme již dříve zmínili, vytvářejí se některá data registru dynamicky při spouštění operačního systému. Jiná data se ukládají na disk, takže je lze použít při každém spuštění počítače. Dynamicky vytvářená data nejsou stálá. To znamená, že se při vypnutí systému ztratí. V rámci procesu spouštění například operační systém hledá zařízení a na základě zjištěných výsledků vytváří podklíč HKEY_LOCAL_MACHINE\HARDWARE. Informace uložené v tomto klíči existují pouze v paměti a neukládají se do žádného umístění na disku.

Na druhou stranu data registru uložená na disk jsou trvalá. Když systém vypnete, zůstávají tato data registru na pevném disku a jsou k dispozici při dalším spuštění systému. Některé z těchto uložených informací jsou velmi důležité, zejména při zotavení z chyby spouštění. Pomocí dat v podklíči HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet lze například systém spustit v poslední známé funkční konfiguraci (Last Known Good Configuration). Jestliže však

byla data registru poškozena, nemusí být tyto informace k dispozici a jedinou možností obnovení může být oprava instalace nebo nová instalace operačního systému.

Systém Windows Server 2008 obsahuje několik integrovaných redundantních mechanismů a pojistek, které chrání systém a zajišťují, že jedna vadná část dat neznemožní načtení celého registru. V prvé řadě není registr zapsán do jediného souboru. Místo toho se ukládá do několika souborů, které se označují jako podregistry. Podregistry se dělí do šesti hlavních typů. Každý z nich přitom reprezentuje skupinu klíčů a hodnot. Většina podklíčů je na disku uložena v adresáři %SystemRoot%\System32\Config. V tomto adresáři se nacházejí následující soubory podregistru:

- .DEFAULT, který odpovídá podklíči HKEY_USERS\.DEFAULT
- SAM, který odpovídá podklíči HKEY_LOCAL_MACHINE\SAM
- SECURITY, který odpovídá podklíči HKEY_LOCAL_MACHINE\SECURITY
- SOFTWARE, který odpovídá podklíči HKEY_LOCAL_MACHINE\SOFTWARE
- SYSTEM, který odpovídá podklíči HKEY_LOCAL_MACHINE\SYSTEM

Zbývající soubory podregistru jsou uloženy v adresářích jednotlivých uživatelských profilů pod výchozími názvy Ntuser.dat. V praxi se jedná o soubory podregistru, které jsou načteny do registru a umožňují nastavit ukazatel na kořenový klíč HKEY_CURRENT_USER. Když není k systému přihlášen žádný uživatel, je do registru načten uživatelský profil výchozího uživatele. Po přihlášení konkrétního uživatele je do registru načten jeho uživatelský profil.



**POZNÁMKA**

Nezmínili jsme kořenové klíče HKEY_CURRENT_CONFIG a HKEY_CLASSES_ROOT. Data klíče HKEY_CURRENT_CONFIG na disku pocházejí z podklíče, ze kterého je vytvořen: HKEY LOCAL MACHINE \SYSTEM\CurrentControlSet\Hardware Profiles\Current. Podobně data klíče HKEY_CLASSES_ROOT na disku jsou načtena z podklíčů HKEY LOCAL MACHINE\SOFTWARE\Classes a HKEY_CURRENT_USER\SOFTWARE\Classes.

Každý soubor podregistru má přidruženy soubory protokolu. Platí to dokonce i pro soubor Ntuser.dat. Systém Windows Server 2008 pomocí souborů protokolu chrání registr při aktualizacích. Když má dojít ke změně souboru podregistru, operační systém zapíše změnu do souboru protokolu a uloží tento protokol na disk. Operační systém pak pomocí protokolu změn zapíše změny do vlastního souboru podregistru. Pokud by operační systém havaroval během zápisu změn do souboru podregistru, bylo by pomocí souboru protokolu později možné změnu vrátit a obnovit předchozí konfiguraci souboru podregistru.

**DO DETAILU**

**Obnovení čistého registru v systému Windows Server 2008**

Když podrobně prozkoumáte složku %SystemRoot%\System32\Config, naleznete zde několik souborů s příponou .sav. Tyto soubory reprezentují stav registru po instalaci. Pokud jste někdy uvažovali nad tím, jak může systém Windows Server 2008 obnovit stav registru po čisté instalaci, když snížíte úroveň řadiče domény, naleznete odpověď v těchto souborech. Když server načte tyto soubory do registru a poté je zapíše na disk místo původních souborů podregistru, přejde zpět do stavu s čistým registrem, v jakém se nacházel po instalaci.

## Typy dostupných dat registru

Když přejdete na nejnižší úroveň registru, můžete zobrazit vlastní položky hodnot. Každá položka hodnoty má přidružen svůj název, datový typ a hodnotu. Položky hodnot mají sice teoretický limit velikosti 1 024 kB, ale většina položek hodnot je menší než 1 kB. Mnohé položky hodnot ve skutečnosti obsahují jen několik datových bitů. Typ uložených informací závisí na datovém typu položky hodnoty.

K definovaným datovým typům patří:

- **REG_BINARY** – binární data bez jakéhokoli formátování či zpracování. Binární data lze zobrazit několika způsoby, k nimž patří standardní binární a hexadecimální zobrazení. Při prohlížení binárních dat se někdy zobrazí jak hexadecimální hodnoty, tak textové znaky, které jsou těmito hodnotami definovány.
- **REG_DWORD** – binární datový typ, ve kterém jsou 32bitové celočíselné hodnoty uloženy jako hexadecimální položky s délkou čtyř bajtů. Datový typ REG_DWORD se často používá při sledování hodnot, které lze inkrementovat, čtyřbajtových stavových kódů nebo logických příznaků. U logických příznaků znamená hodnota 0, že příznak je vypnutý (false), a hodnota 1 symbolizuje, že příznak je zapnutý (true).
- **REG_QWORD** – binární datový typ, ve kterém jsou 64bitové celočíselné hodnoty uloženy jako hexadecimální položky s délkou osmi bajtů. Datový typ REG_QWORD se často používá při sledování hodnot, které lze inkrementovat, osmibajtových stavových kódů nebo logických příznaků. U logických příznaků znamená hodnota 0, že příznak je vypnutý (false), a hodnota 1 symbolizuje, že příznak je zapnutý (true).
- **REG_SZ** – řetězec znaků Unicode s pevnou délkou. Datový typ REG_SZ se používá při ukládání hodnot, které budou číst uživatelé. Může se jednat o jména, popisy atd. a také o uložené cesty v systému souborů.
- **REG_EXPAND_SZ** – řetězec s proměnnou délkou. Může obsahovat proměnné prostředí, které jsou rozbaleny, když čte příslušná data operační systém, jeho součásti či služby a také nainstalované aplikace. Proměnné prostředí jsou uzavřeny mezi symboly procent (%), které je oddělují od ostatních hodnot v řetězci. Hodnota %SystemDrive% například odkazuje na proměnnou prostředí SystemDrive. Hodnota datového typu REG_EXPAND_SZ, které definuje použitou cestu, může zahrnovat tuto proměnnou prostředí, jako např. %SystemDrive%\Program Files\Common Files.
- **REG_MULTI_SZ** – řetězec s více parametry, který umožňuje do jedné položky uložit více řetězcových hodnot. Hodnoty jsou od sebe odděleny standardním oddělovačem, aby je bylo možné v případě potřeby načíst jednotlivě.
- **REG_FULL_RESOURCE_DESCRIPTOR** – hodnota se zakódovaným popisovačem prostředků, což může být například seznam prostředků použitých ovladačem zařízení nebo hardwarovou komponentou. Hodnoty datového typu REG_FULL_RESOURCE_DESCRIPTOR jsou přidruženy k hardwarovým komponentám, např. k hlavním procesorům počítače, matematickým koprocesorům nebo multifunkčním adaptérům.

V registru se nejčastěji setkáte s datovými typy REG_SZ a REG_DWORD. Převážná většina položek hodnot má jeden z těchto datových typů. Nejdůležitější informace týkající se těchto datových typů: první z nich se používá se znakovými řetězci a druhý slouží k uložení binárních dat, která jsou normálně reprezentována v hexadecimálním formátu. Pokud potřebujete vytvořit položku hodnoty (obvykle na základě doporučení článku znalostní báze Microsoft

Knowledge Base, když se snažíte vyřešit jisté potíže), postup obvykle obsahuje informaci o tom, který datový typ je nutné použít. Opět se zpravidla jedná o datový typ REG_SZ nebo REG_DWORD.

# Práce s registrem

Systém Windows Server 2008 poskytuje několik nástrojů pro práci s registrem. Hlavní nástroj se samozřejmě nazývá Editor registru (Registry Editor) a spustíte jej tak, že na příkazový řádek nebo do dialogového okna Spustit (Run) zadáte příkaz **regedit** či **regedt32**. Dalším nástrojem pro práci s registrem je příkaz REG. Oba nástroje umožňují zobrazit a spravovat obsah registru. Pamatujte na to, že i když jsou oba nástroje považovány za editory, systém Windows Server 2008 všechny provedené změny okamžitě použije. Každá provedená změna se tedy automaticky projeví v registru, aniž byste ji museli ukládat.

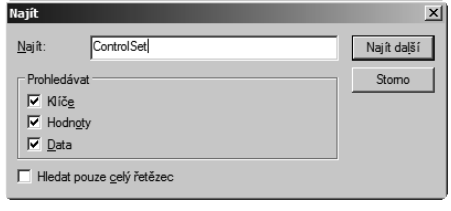
**UPOZORNĚNÍ**

Jako správce máte oprávnění provádět změny ve většině oblastí registru. Díky tomu můžete položky podle potřeby přidávat, měnit a odstraňovat. Než to však uděláte, měli byste vždy nejdříve vytvořit zálohu stavu systému spolu se zálohou registru, jak je popsáno v části „Zálohování a obnovení registru" na straně 282. Tím si uchováte možnost obnovit registr v případě, že při provádění změn dojde k nějaké chybě.



## Prohledávání registru

Mezi běžné úkoly prováděné pomocí Editoru registru patří hledání konkrétního klíče. Klíče, hodnoty a datové položky lze hledat pomocí příkazu Najít (Find) v nabídce Úpravy (Edit) – viz následující obrázek.




Nenechejte se oklamat tím, jak je dialogové okno Najít jednoduché. Možnosti hledání v registru jsou mnohem širší, než by se zdálo. Chcete-li tedy najít požadovanou položku, postupujte takto:

- Funkce Najít (Find) v Editoru registru hledá od aktuálního uzlu směrem vpřed do poslední hodnoty v poslední větvi kořenového klíče. Pokud tedy chcete prohledat celý registr, musíte vybrat uzel Počítač (Computer) v levém podokně dříve, než vyberete příkaz Najít v nabídce Úpravy nebo stisknete klávesy Ctrl+F.
- Text, který chcete vyhledat, zadejte do pole Najít (Find what). Můžete hledat pouze text ve standardním kódování ASCII (American Standard Code for Information Interchange). Hledáte-li tedy datové položky, vyhledá Editor registru zadaný text pouze v řetězcových hodnotách (REG_SZ, REG_EXPAND_SZ a REG_MULTI_SZ).

- Pomocí zaškrtávacích políček v sekci Prohledávat (Look at) můžete ovlivnit, kde bude Editor registru hledat požadovaný text. Je možné hledat názvy klíčů, názvy hodnot a text v datových položkách. Chcete-li vyhledat pouze celé řetězce, nikoli text v rámci delších řetězců, zaškrtněte políčko Hledat pouze celý řetězec (Match Whole String Only).

Když nastavíte příslušné možnosti, spusťte hledání klepnutím na tlačítko Najít další (Find Next). Pokud Editor registru nalezne shodu dříve, než dojde na konec registru, vybere odpovídající položku a zobrazí ji. Jestliže hledáte jinou shodu, pokračujte v hledání od aktuální pozice v registru stisknutím klávesy F3.

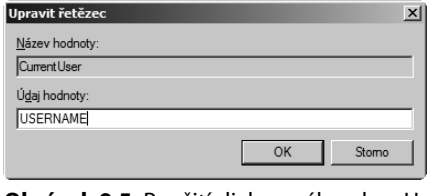
## Úpravy registru

Při práci s klíči a hodnotami v registru se obvykle používají podklíče určitého klíče. Díky tomu lze přidávat podklíče a definovat jejich hodnoty, případě odebírat podklíče s příslušnými hodnotami. Nelze však přidat ani odebrat kořenové klíče ani vložit klíče do kořenového uzlu registru. Výchozí nastavení zabezpečení v rámci určitých podklíčů mohou také znemožnit práci s příslušnými klíči a hodnotami. Ve výchozím nastavení například není možné vytvářet, upravovat ani odebírat klíče či hodnoty v rámci podklíčů HKLM\SAM a HKLM\SECURITY.

### Úpravy hodnot

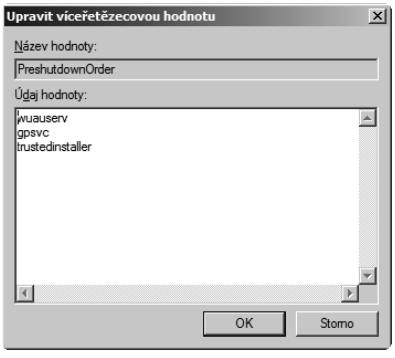
Nejčastější běžnou změnou registru je úprava stávající hodnoty. Článek znalostní báze Knowledge Base může například obsahovat doporučení, abyste změnou hodnoty 0 na 1 povolili určitou funkci systému Windows Server 2008, případně abyste změnili hodnotu 1 na 0 a funkci zakázali. Chcete-li změnit hodnotu, vyhledejte ji v Editoru registru a potom v pravém podokně poklepejte na název hodnoty. Otevře se dialogové okno Upravit (Edit), jehož vzhled závisí na typu dat, která chcete změnit.

Nejčastěji se upravují hodnoty typu REG_SZ, REG_MULTI_SZ a REG_DWORD. Obrázek 9.5 znázorňuje dialogové okno Upravit řetězec (Edit String), které se zobrazí při úpravách hodnot typu REG_SZ. V tomto dialogovém okně obvykle nahradíte stávající hodnotu zobrazenou v poli Údaj hodnoty (Value Data) za hodnotu, kterou potřebujete zadat.




**Obrázek 9.5:** Použití dialogového okna Upravit řetězec

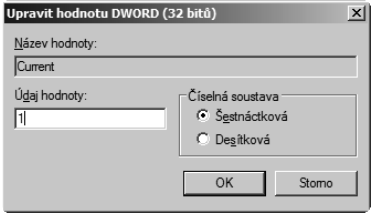
Obrázek 9.6 znázorňuje dialogové okno Upravit víceřetězcovou hodnotu (Edit Multi-String), které se zobrazí při úpravách hodnot typu REG_MULTI_SZ. V tomto případě se jedná o tři samostatné řetězcové hodnoty. Každá hodnota v dialogovém okně je uvedena samostatně na novém řádku, aby bylo možné s hodnotami snáze pracovat. Pokud máte za úkol změnit hodnotu, obvykle budete nahrazovat stávající hodnotu. Přitom byste měli dbát opatrnosti, abyste náhodou neupravili položku, která předchází upravované položce nebo následuje za ní. Jestliže potřebujete přidat hodnotu, začněte psát na novém řádku za poslední hodnotou.




**Obrázek 9.6:** Použití dialogového okna Upravit víceřetězcovou hodnotu

Obrázek 9.7 znázorňuje dialogové okno Upravit hodnotu DWORD (Edit DWORD Value), které se zobrazí při úpravách hodnot typu REG_DWORD. V tomto případě je hodnota zobrazena v hexadecimálním formátu. Formátem dat se obvykle nemusíte zabývat. Stačí zadat novou hodnotu podle pokynů. Pokud například aktuální hodnota představuje příznak, pak hodnota datové položky 1 znamená, že je příznak zapnutý (neboli má hodnotu true). Chcete-li příznak vypnout (nastavit hodnotu false), nahradíte hodnotu 1 hodnotou 0.






**Obrázek 9.7:** Použití dialogového okna Upravit hodnotu DWORD

**POZNÁMKA**

Při práci s Editorem registru je k dispozici schránka systému Windows. To znamená, že můžete používat příkazy Kopírovat, Vyjmout a Vložit stejně jako v jiných programech pro tento systém. Pokud článek ve znalostní bázi Knowledge Base uvádí hodnotu, kterou je obtížné zadat, můžete ji s výhodou zkopírovat do schránky a poté ji vložit do pole Údaj hodnoty (Value Data) dialogového okna Upravit (Edit).

### Přidání klíčů a hodnot

Jak jsme již zmínili, lze ve většině částí registru přidávat nebo odebírat klíče. Výjimky představuje kořenový uzel, kořenové klíče a oblasti registru, kde jsou úpravy zakázány pomocí oprávnění.

Nové klíče je možné přidat jako podklíče vybraného klíče. Otevřete klíč, se kterým chcete pracovat, a poté přidejte podklíč tak, že na klíč klepnete pravým tlačítkem myši a vyberete příkazy Nový a Klíč (New, Key). Editor registru vytvoří nový klíč a vybere jeho název, takže jej můžete nastavit podle potřeby. Výchozí název je Nový klíč #1 (New Key #1).

Novému klíči je automaticky přidělena výchozí položka hodnoty. Datový typ této výchozí hodnoty je REG_SZ. Téměř každý klíč v registru má podobně pojmenovanou položku stejného typu, takže tuto položku hodnoty neodstraňujte. Na položku můžete poklepat a nastavit její hodnotu ve zobrazeném okně Upravit řetězec (Edit String), nebo můžete v rámci vybraného klíče vytvořit dodatečné položky hodnot.

Chcete-li pod klíčem vytvořit další položky hodnot, klepněte na klíč pravým tlačítkem myši a vyberte příkaz Nový (New) následovaný jednou z těchto možností nabídky:

- **Řetězcová hodnota (String Value)** – slouží k zadání řetězce znaků Unicode s pevnou délkou; má datový typ REG_SZ
- **Binární hodnota (Binary Value)** – slouží k zadání binárních dat bez jakéhokoli formátování či zpracování; má datový typ REG_BINARY
- **Hodnota DWORD (32bitová) – DWORD (32-bit) Value** – umožňuje zadat binární datový typ, ve kterém jsou uloženy čtyřbajtové celočíselné hodnoty; má datový typ REG_DWORD
- **Hodnota QWORD (64bitová) – QWORD (64-bit) Value** – umožňuje zadat binární datový typ, ve kterém jsou uloženy osmibajtové celočíselné hodnoty; má datový typ REG_QWORD
- **Víceřetězcová hodnota (Multi-String Value)** – umožňuje zadat řetězec s více parametry; má datový typ REG_MULTI_SZ
- **Rozšiřitelná řetězcová hodnota (Expandable String Value)** – umožňuje zadat řetězec s proměnnou délkou. Ten může obsahovat proměnné prostředí, které jsou rozbaleny při čtení dat; má datový typ REG_EXPAND_SZ

Vytvoříte-li novou hodnotu, přidáte ji do vybraného klíče a pojmenujete ji výchozím názvem Nová hodnota #1, Nová hodnota #2 (New Value #1, New Value #2) atd. Název hodnoty je vybrán pro úpravy, abyste jej mohli okamžitě změnit. Jakmile název hodnoty změníte, můžete poklepáním na tento název upravit data hodnoty.

### Odebrání klíčů a hodnot

Klíče a hodnoty lze z registru odebrat snadno, ale neměli byste to nikdy dělat bez pečlivého zvážení možných důsledků. Klíč nebo hodnotu lze odstranit tak, že je vyberete a poté stisknete klávesu Delete. Editor registru požádá o potvrzení odstranění. Jakmile operaci potvrdíte, je hodnota z registru trvale odstraněna. Pamatujte na to, že když odeberete klíč, odebere Editor registru všechny podklíče a hodnoty přidružené k tomuto klíči.

## Úpravy registru ve vzdáleném počítači

Registr vzdáleného počítače můžete upravit, aniž byste se k němu museli přihlásit místně. V nabídce Soubor (File) Editoru registru vyberte příkaz Připojit síťový registr (Connect Network Registry) a poté v dialogovém okně pro výběr počítače určete počítač, se kterým chcete pracovat. Ve většině případů stačí zadat název vzdáleného počítače a klepnout na tlačítko OK. V případě zobrazení výzvy může být nutné zadat uživatelské jméno a heslo k účtu, který má oprávnění pro přístup ke vzdálenému počítači.

Jakmile se připojíte, zobrazí se pod ikonou Počítač (Computer) v levém podokně Editoru registru nová ikona vzdáleného počítače. Poklepáním na tuto ikonu získáte přístup k fyzickým kořenovým klíčům ve vzdáleném počítači (HKEY_LOCAL_MACHINE a HKEY_USERS).

Logické kořenové klíče nejsou k dispozici, protože se buď vytvářejí dynamicky nebo se jedná o pouhé ukazatele na podmnožiny informací v rámci klíčů HKEY_LOCAL_MACHINE a HKEY_USERS. Poté můžete upravit registr počítače podle potřeby. Po dokončení můžete vybrat příkaz Odpojit síťový registr (Disconnect Network Registry) v nabídce Soubor (File) a zvolit počítač, od kterého se chcete odpojit. Editor registru pak uzavře registr ve vzdáleném počítači a přeruší připojení..

Při práci se vzdálenými počítači můžete také načítat a uvolňovat podregistry postupem, který je popsán v oddíle „Načítání a uvolňování souborů podregistru" na straně 281. Možná přemýšlíte nad tím, k čemu je tato funkce dobrá. Otevření konkrétního podregistru (např. podregistru, který odkazuje na uživatelský profil určitého uživatele) můžete potřebovat například tehdy, pokud daný uživatel nastavil neplatný režim zobrazení a nemůže nyní s počítačem místně pracovat. Když načtete data profilu daného uživatele, můžete úpravou registru problém vyřešit a poté uložit změny, aby se uživatel mohl opět k systému přihlásit.

## Import a export dat registru



Někdy se můžete dostat do situace, kdy je nutné nebo vhodné zkopírovat celý registr nebo jeho část do souboru. Pokud jste například nainstalovali službu nebo komponentu, která vyžaduje rozsáhlou konfiguraci, můžete tuto konfiguraci chtít přenést do jiného počítače, abyste ji nemuseli opakovat ručně. V tomto případě je tedy možné nainstalovat základní službu či komponentu do nového počítače, poté exportovat nastavení registru pro aplikaci z předchozího počítače, zkopírovat toto nastavení do nového počítače a nakonec je importovat do registru, aby byla služba či komponenta nakonfigurována správně. Tento postup samozřejmě funguje jen v případě, že je kompletní konfigurace služby nebo komponenty umístěna v registru. Nyní však nejspíše vidíte, jak užitečný může být import či export dat registru.

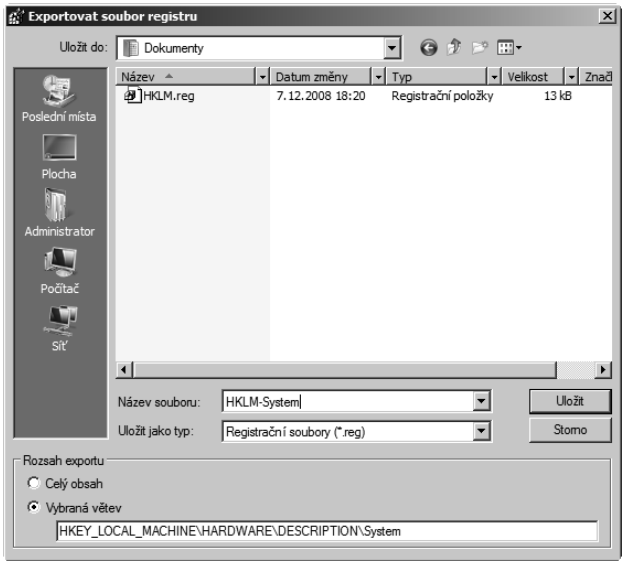
Pomocí Editoru registru lze data registru importovat a exportovat poměrně snadno. Týká se to celého registru, větví dat vycházejících z konkrétního kořenového klíče i jednotlivých podklíčů a hodnot, které obsahují. Při exportu dat vytvoříte soubor typu .reg, který obsahuje určená data registru. Tento soubor registru je skript, který můžete poté načíst zpět do registru stejného nebo jiného počítače tak, že jej importujete.

**POZNÁMKA**

Vzhledem k tomu, že skript registru je uložen ve standardním textovém formátu, můžete jej zobrazit a v případě potřeby i upravit v libovolném běžném textovém editoru. Pamatujte však, že poklepáním na soubor .reg spustíte Editor registru, který zobrazí dotaz, zda chcete data importovat do registru. Pokud vám to nevyhovuje, uložte data do souboru s příponou .hiv. Poklepáním na soubor s touto příponou se totiž Editor registru nespustí. Soubory s příponou .hiv je nutné importovat ručně (případně můžete změnit příponu souboru na .reg, když se chystáte data použít).

Chcete-li exportovat data registru, klepněte pravým tlačítkem na větev nebo klíč, který chcete exportovat, a vyberte příkaz Exportovat (Export). Můžete také klepnout pravým tlačítkem myši na kořenový uzel počítače, který používáte (např. Počítač – Computer v případě místního počítače), a exportovat celý registr. V obou případech se zobrazí dialogové okno Exportovat soubor registru (Export Registry File), které je znázorněno na obrázku 9.8. V seznamu Uložit do (Save in) zvolte umístění pro uložení souboru .reg a zadejte název souboru. Panel Rozsah registru (Export Range) označuje vybranou větev registru, která bude exportována. Tuto hodnotu

můžete podle potřeby změnit, také můžete klepnutím na přepínač Celý obsah (All) exportovat celý registr. Potom vytvořte soubor typu .reg klepnutím na tlačítko Uložit (Save).




**Obrázek 9.8:** Export dat registru do souboru .reg, aby je bylo možné uložit a v případě potřeby importovat do stejného nebo jiného počítače

**DO DETAILU**

**Rychlý export celého registru**

Chcete-li exportovat celý registr, zadejte na příkazový řádek **regedit /e SouborNaDisku**, kde *SouborNaDisku* je úplná cesta do umístění, kam chcete kopii registru uložit. Pokud například chcete kopii registru uložit do umístění C:\Podniksvr06 regdata.reg, zadejte příkaz **regedit /e C:\podniksvr06-regdata.reg**.

Tento postup můžete také rozšířit a rychle zjistit konkrétní hodnoty registru, které operační systém mění při změnách nastavení systému nebo aplikace. Nejdříve otevřete aplikaci nebo systémový nástroj, se kterým chcete pracovat, a současně okno příkazového řádku. Dále exportujte registr dříve, než provedete změnu, kterou chcete sledovat. Aniž byste provedli cokoli jiného, ihned poté proveďte změnu, kterou chcete sledovat. Exportujte registr do jiného souboru pomocí okna příkazového řádku, které jste otevřeli na začátku celého postupu. Nakonec porovnejte soubory nástrojem na porovnání souborů (fc.exe). Jestliže jste například uložili původní registr do souboru orig.reg a změněný registr do souboru novy.reg, můžete na příkazový řádek zadat následující příkaz, který zapíše změny do souboru s názvem zmeny.txt: **fc /u orig.reg novy.reg > zmeny.txt**. Když soubor zmeny.txt otevřete v textovém editoru, uvidíte porovnání souborů registru a přesné rozdíly mezi nimi.

Import dat registru přidá obsah souboru skriptu do registru počítače, se kterým pracujete. Přitom jsou vytvořeny klíče a hodnoty, které zatím neexistují, a stávající klíče a hodnoty jsou přepsány. Data registru lze importovat jedním ze dvou způsobů. Můžete poklepat na soubor typu .reg. Tím spustíte Editor registru, který zobrazí dotaz, zda chcete data importovat. Případně můžete zvolit příkaz Importovat (Import) v nabídce Soubor (File) a poté v dialogo-

vém okně Importovat soubor registru (Import Registry File) vybrat a otevřít datový soubor registru, který chcete načíst.

**DO DETAILU**

**Distribuce změn registru pomocí postupů pro export a import**

Postupy exportu a importu umožňují snadno distribuovat změny registru uživatelům. Můžete například exportovat podklíč s důležitou změnou konfigurace a poté odeslat příslušný soubor .reg pomocí e-mailu uživatelům, kteří pak mohou soubor importovat pouhým poklepáním. Alternativně můžete zkopírovat soubor typu .reg na síťovou sdílenou složku, kde ji uživatelé mohou otevřít a použít. V obou případech máte k dispozici snadný a rychlý způsob, jak šířit změny registru. Oficiálně se však distribuce změn registru tímto způsobem nedoporučuje, protože s tímto postupem souvisejí potenciální bezpečnostní problémy. Upřednostňovaným postupem je distribuce změn registru pomocí zásad skupin, jak je popsáno v části 5.

## Načítání a uvolňování souborů podregistru



Stejně jako je někdy nutné data registru importovat nebo exportovat, je občas nutné pracovat s jednotlivými soubory podregistru. Nejčastějším důvodem (jak jsme již vysvětlili) je požadavek na úpravu uživatelského profilu kvůli problému, který uživateli znemožňuje přístup k jeho systému. V tomto případě byste do Editoru registru načetli uživatelův soubor Ntuser.dat a poté provedli potřebné změny. Další důvod pro tuto operaci může být změna konkrétní části registru ve vzdáleném systému. Jestliže například potřebujete opravit část registru, můžete související soubor podregistru načíst do registru jiného počítače a poté problém opravit ve vzdáleném počítači.

Načítání a uvolňování podregistrů se týká pouze klíčů HKEY_LOCAL_MACHINE a HKEY_USERS a tyto akce je možné provést pouze při výběru jednoho z těchto kořenových klíčů. Místo toho, abyste vybraný kořenový klíč nahradili, se načtený podregistr objeví jako podklíč daného kořenového klíče. Klíče HKEY_LOCAL_MACHINE a HKEY_USERS samozřejmě umožňují vytvářet všechny logické kořenové klíče, které se v systému používají, takže v praxi můžete pracovat s libovolnou částí registru.

Jakmile v Editoru registru vyberete klíč HKEY_LOCAL_MACHINE nebo HKEY_USERS můžete načíst podklíč pro aktuální nebo jiný počítač tak, že v nabídce Soubor (File) vyberete příkaz Načíst podregistr (Load Hive). Editor registru pak požádá o zadání umístění a názvu dříve uloženého souboru podregistru. Vyberte soubor a klepněte na tlačítko Otevřít (Open). Poté zadejte název klíče, pod kterým chcete podregistr umístit po načtení do registru aktuálního systému, a klepněte na tlačítko OK.

**POZNÁMKA**

Nelze pracovat se soubory podregistru, které aktuálně používá operační systém nebo jiný proces. Můžete však vytvořit kopii podregistru a poté s ní pracovat. Na příkazovém řádku zadejte příkaz **reg save** následovaný zkráceným názvem kořenového klíče, který chcete uložit, a názvem souboru, do kterého bude podregistr uložen. Můžete například pomocí příkazu **reg save hkcu c:\aktual-hkcu.hiv** uložit klíč HKEY_CURRENT_USER do souboru s názvem Aktual-hkcu.hiv na jednotce C. I když lze uvedeným způsobem uložit logické kořenové klíče (HKCC, HKCR, HKCU), umožňuje tento postup v případě klíčů HKLM a HKU uložit pouze podklíče.

Když dokončíte práci s podregistrem, měli byste jej uvolnit, abyste jej odstranili z paměti. Uvolnění podregistru neuloží provedené změny. Stejně jako u jiných úprav registru platí, že změny se použití automaticky, aniž byste je museli ukládat. Chcete-li podklíč uvolnit, vyberte jej a z nabídky Soubor (File) vyberte příkaz Uvolnit podregistr (Unload Hive). Po zobrazení výzvy k potvrzení klepněte na tlačítko Ano (Yes).

## Práce s registrem pomocí příkazového řádku

K používání registru z příkazového řádku slouží příkaz REG. Příkaz REG je spuštěn pomocí oprávnění aktuálního uživatele a můžete pomocí něj přistupovat k registru v místních i vzdálených systémech. Stejně jako v případě Editoru registru lze ve vzdálených počítačích pracovat pouze s klíči HKEY_LOCAL_MACHINE a HKEY_USERS. Tyto klíče samozřejmě umožňují vytvářet všechny logické kořenové klíče, které se v systému používají, takže v praxi můžete pracovat s libovolnou části registru vzdáleného systému.

Příkaz REG poskytuje odlišné dílčí příkazy pro jednotlivé úlohy registru. Jedná se o následující příkazy:

- **REG ADD** – přidá do registru nový podklíč nebo položku hodnoty.
- **REG COMPARE** – porovná podklíče nebo položky hodnoty registru.
- **REG COPY** – zkopíruje položku registru do zadané cesty klíče v místním nebo vzdáleném systému.
- **REG DELETE** – odstraní podklíč nebo položky hodnot z registru.
- **REG EXPORT** – exportuje data registru a zapíše je do souboru.

**POZNÁMKA**

Tyto soubory mají stejný formát jako soubory exportované z Editoru registru. Obvykle jsou však uloženy s příponou .hiv, takže se poklepáním na tyto soubory Editor registru nespustí.

- **REG IMPORT** – importuje data registru a přitom buď vytvoří nové klíče a položky hodnot, nebo stávající klíče a položky hodnot přepíše.
- **REG LOAD** – načte soubor podregistru.
- **REG QUERY** – vypíše položky hodnot pod klíčem a názvy případných podklíčů.
- **REG RESTORE** – zapíše uložené podklíče a položky zpět do registru.
- **REG SAVE** – uloží kopii uvedených podklíčů a položek hodnot do souboru.
- **REG UNLOAD** – uvolní soubor podregistru.

Syntaxi pro použití těchto příkazů zjistíte zadáním příkazu **reg** následovaným názvem dílčího příkazu, pro který získat informace, a znaků **/?**. Chcete-li se například dozvědět více o příkazu REG ADD, zadejte **reg add /?** na příkazový řádek.

# Zálohování a obnovení registru

Nyní by mělo být zcela jasné, že registr je velmi důležitý a je nutné jej chránit. Dokonce lze říci, že registr by měl být součástí každého plánu zálohování a obnovení. K zálohování a obnovení registru se obvykle nepoužívá Editor registru. Slouží k tomu nástroj Zálohování serveru (Windows Server Backup), případně upřednostňovaný zálohovací nástroj jiného dodavatele.

V každém případě můžete účinně minimalizovat výpadky a zajistit, že lze v případě poškození registru obnovit systém.

Zálohu celého registru lze velmi snadno vytvořit z příkazového řádku. Stačí zadat příkaz **regedit /e *SouborNaDisku***, kde *SouborNaDisku* představuje úplnou cestu do umístění, kam chcete data registru uložit. Poté můžete uložit kopii registru do souboru C:\Backups\Regdata.reg zadáním příkazu **regedit /e c:\backups\regdata.reg**. Tímto způsobem získáte úplnou zálohu registru.

Je také možné snadno vytvořit zálohy jednotlivých klíčů registru. K tomu je určen příkaz REG SAVE. Zadejte příkaz **reg save** následovaný zkráceným názvem kořenového klíče, který chcete uložit, a požadovaným názvem souboru. Příkazem **reg save hkcu c:\backups\hkcu.hiv** můžete například uložit klíč HKEY_CURRENT_USER do souboru v adresáři C:\Backups. Opět platí, že i když lze uvedeným způsobem uložit logické kořenové klíče (HKCC, HKCR, HKCU), umožňuje tento postup v případě klíčů HKLM a HKU uložit pouze podklíče.

Nyní tedy umíte rychle a snadno zálohovat data registru. Nemáte však k dispozici zaručený způsob, jak obnovit systém v případě, že je registr poškozen a systém nelze spustit. Je to zčásti způsobeno tím, že nelze nijak spustit systém a získat přístup k datům registru.

V systému Windows Server 2008 lze vytvořit zálohu stavu systému, která umožňuje obnovit registr a vrátit systém do spustitelného stavu. Zálohy stavu systému zahrnují klíčové systémové soubory, které jsou nutné k obnovení místního systému, a také data registru. Všechny počítače mají data stavu systému, která je nutné zálohovat spolu s dalšími soubory, aby bylo možné obnovit kompletní funkční systém.

Data stavu systému se zpravidla zálohují během normální (úplné) zálohy zbytku dat v systému. Pokud tedy provádíte úplné obnovení serveru (nikoli opravu), můžete pomocí úplné zálohy systému spolu s daty stavu systému obnovit server beze zbytku. Postupy, jak provádět úplné zálohování a obnovení systému, jsou popsány v kapitole 41, „Zálohování a obnovení".

Můžete však vytvořit i samostatné zálohy stavu systému. Nejrychleji a nejsnáze tyto zálohy získáte nástrojem Wbadmin, který představuje obdobu nástroje Zálohování serveru pro příkazový řádek. Chcete-li vytvořit zálohu stavu systému nástrojem Wbadmin, zadejte na příkazový řádek se zvýšenými oprávněními následující příkaz:

```
wbadmin start systemstatebackup -backuptarget JednotkaÚložiště
```

kde *JednotkaÚložiště* představuje písmeno jednotky umístění úložiště, jako např.:

```
wbadmin start systemstatebackup -backuptarget d:
```

# Údržba registru

Registr je databáze a stejně jako jiné databáze funguje nejlépe, když je optimalizovaný. Registr můžete optimalizovat tak, že omezíte objem balastu a informací, které obsahuje. To znamená, že je vhodné odinstalovat nepotřebné systémové komponenty, služby a aplikace. Komponenty, služby a aplikace můžete odinstalovat například pomocí nástroje Odinstalovat nebo změnit program (Uninstall or Change a Program) v ovládacích panelech. Tento nástroj umožňuje bezpečně odebrat součásti systému Windows a související služby a také aplikace nainstalované pomocí Instalační služby Windows Installer. V ovládacích panelech klepněte na odkaz

Odinstalovat program (Uninstall a Program) pod nadpisem Programy (Programs). Zobrazí se okno nástroje Odinstalovat nebo změnit program (Uninstall or Change a Program).

Většina aplikací zahrnuje nástroje pro odinstalování, které se rovněž snaží bezpečně a efektivně odebrat aplikace, jejich data a nastavení registru. Někdy však aplikace buď instalační nástroj neobsahuje nebo z určitého důvodu kompletně neodstraní svá nastavení registru. V těchto případech se hodí použít nástroje na údržbu registru.

Z webu Stažení softwaru si můžete stáhnout sadu nástroje Windows Installer Clean Up Utility. Tento balíček ke stažení obsahuje několik souborů a také pomocnou aplikaci s názvem Windows Installer Zapper. Nástroj Windows Installer Clean Up Utility volá nástroj Windows Installer Zapper, který následně provádí čisticí operace pro údaje správy konfigurace Instalační služby Windows Installer. S nástrojem Windows Installer Zapper je také možné pracovat přímo, ačkoli to nelze doporučit začínajícím správcům.

Než si tyto nástroje stáhnete a začnete je používat, měli byste si přečíst článek znalostní báze Microsoft Knowledge Base číslo 29031 (*http://support.microsoft.com/kb/290301/en-us*). Tento článek také obsahuje odkaz na stažení balíčku instalačního programu. Jakmile si balíček instalačního programu stáhnete, klepněte na něj pravým tlačítkem myši a poté vyberte příkaz Spustit jako správce (Run as Administrator). Při instalaci čisticích nástrojů postupujte podle zobrazených pokynů. Ve složce %SystemDrive%\Program Files\Windows Installer Clean Up naleznete nástroj Windows Installer Clean Up Utility (msicuu.exe), nástroj Windows Installer Zapper (msizap.exe) a soubor readme (readme.txt).

**POZNÁMKA**

Nástroj Windows Installer Zapper je k dispozici ve dvou verzích: MsiZapA.exe je určen pro systémy Windows 95, Windows 98 a Windows ME a program MsiZapU.exe slouží pro všechny ostatní verze systému Windows. Při instalaci nástroje Windows Installer Clean Up Utility nainstaluje instalační program správnou verzi automaticky a přejmenuje spustitelný soubor .exe na Msizap.exe.

Oba nástroje jsou navrženy tak, aby fungovaly s programy, které byly nainstalovány pomocí Instalační služby Windows Installer. Ke svému spouštění vyžadují účty s oprávněními správce. Kromě toho, že tyto nástroje umožňují vymazat nastavení registru pro programy, které jste dříve nainstalovali a pak odinstalovali, můžete pomocí nich obnovit registr do stavu, ve kterém se nacházel před neúspěšnou nebo předčasně ukončenou instalací. Tento postup funguje za předpokladu, že byla aplikace nainstalována pomocí Instalační služby Windows Installer.

## Použití nástroje Windows Installer Clean Up Utility

Nástroj Windows Installer Clean Up Utility odstraňuje nastavení registru pro aplikace, které byly nainstalovány pomocí Instalační služby Windows Installer. Nejužitečnější je v případech, kdy chcete registr vyčistit od pozůstatků aplikací, které byly odinstalovány pouze zčásti nebo jejichž odinstalování se nezdařilo. Hodí se také při čištění aplikací, které nelze odinstalovat nebo znovu nainstalovat z důvodu neúplného nebo poškozeného nastavení registru. Nástroj však není určen k tomu, aby nahradil odinstalační program. Neodstraní totiž soubory ani zástupce aplikace. Budete-li chtít příslušnou aplikaci používat, budete ji muset znovu nainstalovat.

**POZNÁMKA**

Pamatujte, že součástí registru je profil aktuálního uživatele. Nástroj Windows Installer Clean Up Utility proto z tohoto profilu odebere uživatelsky specifická instalační data. Neodstraní však tyto údaje z jiných profilů.

Pokud jste již spustili balíček instalačního programu, můžete tento nástroj spustit postupným klepnutím na tlačítko Start, příkaz Všechny programy (All Programs) a položku Windows Installer Clean Up. Když se zobrazí dialogové okno nástroje Windows Installer Clean Up Utility, vyberte program či programy, které chcete vyčistit, a klepněte na tlačítko Odebrat (Remove). Nástroj Windows Installer Clean Up Utility uchovává soubor protokolu, do něhož zaznamenává aplikace, které uživatelé odstranili tímto způsobem. Protokol je uložen v adresáři %SystemDrive%\Users*UživatelskéJméno*\AppData\Local\Temp a nazývá se Msicuu.log.

**POZNÁMKA**

Nástroj Windows Installer Clean Up Utility je grafické uživatelské rozhraní nástroje Windows Installer Zapper, který si popíšeme v následujícím oddílu. Použijete-li tento nástroj, je spuštěn nástroj Windows Installer Clean Up Utility s parametrem /T pro odstranění položek registru aplikace. Výhodou tohoto postupu je vytvoření souboru protokolu, který se v případě nástroje Windows Installer Zapper nepoužívá.

**UPOZORNĚNÍ**

Nástroj Windows Installer Clean Up Utility byste měli používat pouze jako poslední možnost. Nespouštějte jej, pokud lze program odinstalovat jinými způsoby.



## Použití nástroje Windows Installer Zapper

Windows Installer Zapper (Msizap.exe) je pokročilý nástroj pro příkazový řádek, který odstraňuje nastavení registru pro aplikace, které byly nainstalovány pomocí Instalační služby Windows Installer. Podobně jako nástroj Windows Installer Clean Up Utility jej můžete využít při čištění aplikací, které byly odinstalovány částečně nebo které se odinstalovat nepodařilo. Hodí se také při čištění aplikací, které nelze odinstalovat nebo znovu nainstalovat z důvodu neúplného nebo poškozeného nastavení registru. Kromě toho dovoluje odebrat nastavení registru, která souvisejí s neúspěšnými instalacemi nebo neúspěšnými pokusy o vrácení instalace. Nástroj také umožňuje opravit chyby, ke kterým dochází, když je současně spuštěno více instancí instalačního programu. Může také vyřešit situace, kdy instalační program nelze spustit. Vzhledem k tomu, že může program způsobit závažné problémy operačního systému, měli by s ním pracovat pouze zkušení správci.

Nástroj Windows Installer Zapper naleznete ve složce %SystemDrive%\Program Files\Windows Installer Clean Up. Dále je uvedena úplná syntaxe programu Windows Installer Zapper:

```
msizap [*] [!] [A] [M] [P] [S] [W] [T] [G] [AppToZap]
```

kde

- **AppToZap** – určuje kód produktu aplikace nebo cestu k souboru programu Instalační služby Windows Installer (.msi) dané aplikace.

- * – odstraní z počítače všechny konfigurační informace Instalační služby Windows Installer, včetně údajů uložených v registru a na disku. Parametr je nutné použít s příznakem ALLPRODUCTS.
- **!** – vypne varovná upozornění se žádostí o potvrzení akcí.
- **A** – poskytne správcům oprávnění Úplné řízení (Full Control) k příslušným datům Instalační služby Windows Installer. Data lze tedy odstranit i v případě, že k nim správce nemá výslovný přístup.
- **M** – odstraní informace registru související se spravovanými opravami.
- **P** – odstraní informace registru související s aktivními instalacemi.
- **S** – odstraní informace registru uložené kvůli možnosti vrácení do předchozího stavu.
- **T** – používá se při určení aplikace, která bude vyčištěna.
- **W** – vyhledá ve všech uživatelských profilech data, která mají být odstraněna.
- **G** – odebere osamocené soubory Instalační služby Windows Installer, které byly uloženy do mezipaměti pro všechny uživatele.

**UPOZORNĚNÍ**

Nástroj Windows Installer Zapper byste měli používat pouze jako poslední možnost. Nespouštějte jej, pokud lze program odinstalovat jinými způsoby.

### Odebrání nastavení registru pro neúspěšné aktivní instalace

Někdy dojde k chybě při instalaci aplikací nebo po instalaci. V průběhu instalace aplikací je v registru vytvořen klíč InProgress, který je umístěn v podklíči HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer. V případě, že instalace neskončí úspěšně, systém někdy tento klíč nedokáže upravit nebo odebrat. Pokud k tomu dojde, je instalační program aplikace při dalším pokusu o spuštění ukončen s chybou. Spustíte-li nástroj Windows Installer Zapper s parametrem P, vymažete tím klíč InProgress. Poté by mělo být možné instalační program aplikace znovu spustit.

Po instalaci se aplikace spoléhají na své nastavení registru, kam ukládají konfigurační údaje. Pokud jsou tato nastavení poškozena nebo dojde k poškození instalace, nelze aplikaci spustit. Některé programy mají nástroj pro opravu, který můžete spustit pouhým opakovaným spuštěním instalace. Během obnovy se Instalační služba Windows Installer může pokusit o zápis změn do registru, aby instalaci opravila, nebo ji vrátila zpět a obnovila původní stav systému. Jestliže se proces z nějakého důvodu nezdaří, může registr obsahovat nežádoucí nastavení aplikace. Chcete-li vymazat data pro vrácení aktivní instalace, spusťte nástroj Windows Installer Zapper s parametrem S. Data vrácení jsou uložena v klíči HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Rollback.

Každá spuštěná instalace má také data vrácení, takže se parametry P a S obvykle používají současně. To znamená, že byste na příkazový řádek se zvýšenými oprávněními zadali příkaz **msizap ps**.

### Odebrání částečných nebo poškozených nastavení jednotlivých aplikací

Když nelze aplikaci úspěšně odinstalovat, můžete se pokusit vyčistit její nastavení z registru pomocí nástroje Windows Installer Zapper. K tomu potřebujete znát kód produktu aplikace nebo úplnou cestu k souboru Instalační služby Windows Installer, pomocí nějž byla aplika-

ce nainstalována. Soubor instalační služby má příponu .msi a obvykle jej naleznete v jednom z instalačních adresářů aplikace.

Poté můžete zadat příkaz **msizap t** následovaný kódem produktu nebo cestou k souboru .msi. Pokud má například soubor instalační služby umístění C:\Apps\KDC\KDC.msi, můžete na příkazový řádek zadat příkaz **msizap t c:\apps\kdc\kdc.msi** a tím vymazat nastavení aplikace. Vzhledem k tomu, že součástí registru je profil aktuálního uživatele, jsou z tohoto profilu odebrána uživatelsky specifická nastavení dané aplikace. Chcete-li tato nastavení vymazat ze všech uživatelských profilů v systému, přidejte k příkazu parametr W, jako např. **msizap wt c:\apps\kdc\kdc.msi**.

# Zabezpečení registru

Registr je kritickou částí operačního systému. Poskytuje určité omezené zabezpečení, které snižuje riziko, že dojde k neúmyslné změně nebo odstranění důležitých nastavení. Některé oblasti registru jsou dále dostupné pouze určitým uživatelům. Podklíče HKLM\SAM a HKLM\SECURITY jsou například k dispozici pouze uživateli LocalSystem. Toto zabezpečení však nemusí v některých případech stačit k tomu, aby zabránilo neautorizovanému přístupu k registru. Z tohoto důvodu může být vhodné nastavit přísnější řízení přístupu oproti výchozím oprávněním, což můžete provést přímo v rámci registru. Je také možné řídit vzdálený přístup k registru a konfigurovat auditování přístupu.

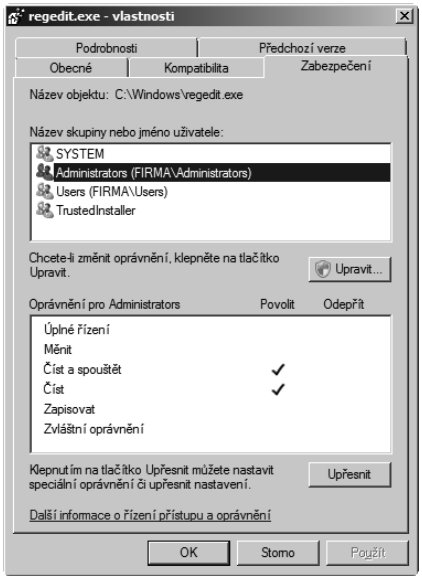


## Zabránění přístupu k nástrojům registru

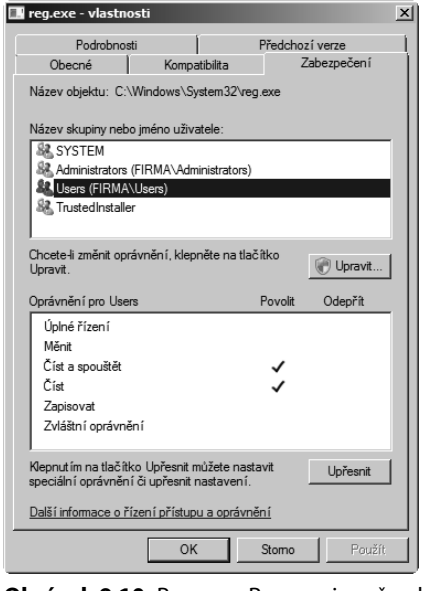
Chcete-li chránit registr před neautorizovaným přístupem, je jeden z nejlepších způsobů založen na tom, že uživatelé nemohou k registru vůbec přistupovat. V případě serveru to obnáší přísnou kontrolu fyzického zabezpečení, kdy se mohou místně přihlásit pouze správci. U jiných systémů, kde není praktické uživatelům zakázat místní přihlášení k serveru, můžete nakonfigurovat oprávnění k programům Regedit.exe a Reg.exe, aby byly tyto soubory lépe zabezpečeny. Lze také ze systému odebrat Editor registru a příkaz REG, ale tím můžete způsobit jiné potíže a zkomplikovat správu systému, zejména pokud zároveň zabráníte vzdálenému přístupu k registru.

Pokud chcete upravit oprávnění k Editoru registru, otevřete složku %SystemRoot%, klepněte pravým tlačítkem myši na soubor Regedit.exe a vyberte příkaz Vlastnosti (Properties). V dialogovém okně vlastností nástroje Regedit klepněte na kartu Zabezpečení (Security), která je znázorněna na obrázku 9.9. Podle potřeby přidejte a odeberte uživatele a skupiny a poté nastavte vhodná oprávnění. Oprávnění fungují stejným způsobem jako u jiných typů souborů. Po výběru objektu lze povolit nebo odepřít konkrétní oprávnění. Podrobnosti naleznete v kapitole 14, „Sdílení souborů a zabezpečení".

Jestliže chcete upravit oprávnění k příkazu REG, otevřete složku %SystemRoot%, klepněte pravým tlačítkem myši na soubor Reg.exe a vyberte příkaz Vlastnosti (Properties). V dialogovém okně vlastností programu Reg klepněte na kartu Zabezpečení (Security). Jak je patrné na obrázku 9.10, mohou tento program ve výchozím nastavení používat správci i uživatelé. Podle potřeby přidejte a odeberte uživatele a skupiny a poté nastavte vhodná oprávnění.




**Obrázek 9.9:** Omezením přístupu k Editoru registru lze zpřísnit kontrolu




**Obrázek 9.10:** Program Reg.exe je určen k tomu, aby s ním pracovali uživatelé i správci, a spouští se z příkazového řádku. To se projevuje v jeho oprávněních.

**POZNÁMKA**

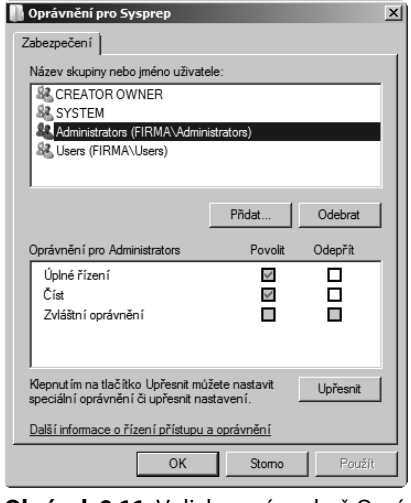
Nezapomněli jsme na nástroj Regedt32. Jedná se pouze o odkaz na nástroj Regedit.exe, takže jeho přístupová oprávnění v praxi nemusíte nastavovat. Oprávnění nástroje Regedit.exe se projeví bez ohledu na to, zda se uživatelé pokusí spustit program Regedt32 nebo Regedit.exe.

## Použití oprávnění ke klíčům registru

Také klíče v rámci registru mají přístupová oprávnění. Místo toho, abyste tato oprávnění upravovali přímo, je vhodné použít příslušnou šablonu zabezpečení, jak je popsáno v kapitole 36, „Správa zásad skupin". Použitím správné šablony zabezpečení uzamknete přístup k registru a nebudete se muset obávat neúmyslných změn, které by zabránily spuštění systému nebo aplikací.

V některých výjimečných situacích však můžete požadovat změnu oprávnění k jednotlivým klíčům registru. Chcete-li to provést, spusťte Editor registru a přejděte na klíč, se kterým potřebujete pracovat. Když klíč naleznete, klepněte na něj pravým tlačítkem myši a vyberte příkaz Oprávnění (Permissions). Případně vyberte klíč a klepněte na příkaz Oprávnění (Permissions) v nabídce Úpravy (Edit). Zobrazí se dialogové okno Oprávnění pro (Permissions for), které je podobné oknu na obrázku 9.11. Oprávnění fungují stejným způsobem jako u souborů. Podle potřeby lze přidat a odebrat uživatele a skupiny. Po výběru objektu lze povolit nebo odepřít konkrétní oprávnění.






**Obrázek 9.11:** V dialogovém okně Oprávnění pro lze nastavit oprávnění ke konkrétním klíčům registru

Mnohá oprávnění se dědí z klíčů vyšší úrovně a nejsou k dispozici. Chcete-li upravit tato oprávnění, musíte otevřít dialogové okno Upřesnit nastavení zabezpečení (Advanced Security Settings) klepnutím na tlačítko Upřesnit (Advanced). Jak je zřejmé z obrázku 9.12, obsahuje dialogové okno Upřesnit nastavení zabezpečení čtyři karty:

- **Oprávnění (Permissions)** – sloupec Zděděno od (Inherited from) na kartě Oprávnění (Permissions) informuje o tom, odkud jsou oprávnění zděděna. Obvykle se jedná

o kořenový klíč větve, se kterou pracujete, jako např. CURRENT_USER. Pomocí tlačítek Přidat (Add) a Upravit (Edit) na kartě Oprávnění můžete nastavit přístupová oprávnění pro jednotlivé uživatele a skupiny. Tabulka 9.2 shrnuje jednotlivá oprávnění, která je možné nastavit.

**UPOZORNĚNÍ**

Dříve než použijete změny klepnutím na tlačítko OK, zvažte, zda je vhodné zrušit zaškrtnutí políčka Zahrnout zděditelné oprávnění z nadřazeného objektu (Include Inheritable Permissions from This Object's Parent). Pokud to neuděláte, změníte oprávnění pro vybraný klíč a všechny jeho podklíče.

- **Auditování (Auditing)** – umožňuje konfigurovat auditování pro vybraný klíč. Akce, které lze auditovat, se shodují s oprávněními uvedenými v tabulce 9.2. Viz „Kořenové klíče registru" na straně 265.
- **Vlastník (Owner)** – zobrazuje aktuálního vlastníka vybraného klíče a umožňuje změnit vlastnictví. Ve výchozím nastavení je ovlivněn pouze vybraný klíč. Pokud však chcete změny použít na všechny podklíče aktuálně vybraného klíče, zaškrtněte políčko Nahradit vlastníka v podřízených kontejnerech a objektech (Replace Owner on Subcontainers and Objects).

**UPOZORNĚNÍ**

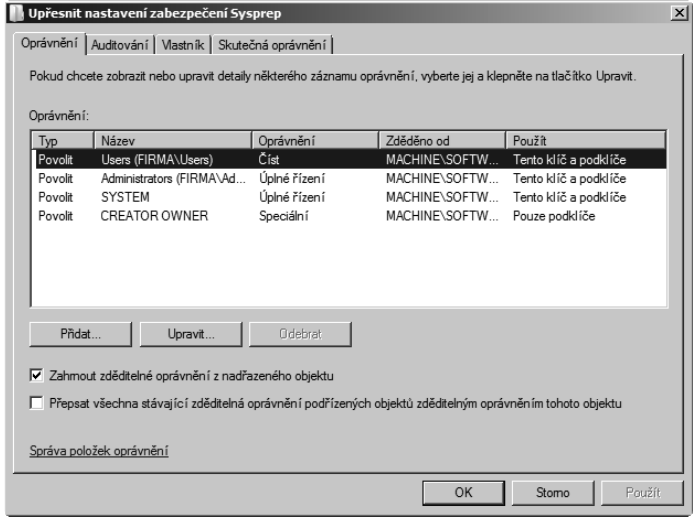
Pokud se chystáte převzít vlastnictví klíčů registru, měli byste rozumět důsledkům tohoto kroku. Změnou vlastnictví můžete neúmyslně zabránit operačnímu systému nebo jiným uživatelům ve spouštění aplikací, služeb nebo komponent aplikací.

- **Skutečná oprávnění (Effective Permissions)** – umožňuje zjistit, která oprávnění by získal určitý uživatel nebo skupina na základě aktuálních nastavení. Jedná se o užitečnou pomůcku, protože změny oprávnění provedené na kartě Oprávnění se projeví teprve po klepnutí na tlačítko OK nebo Použít (Apply).

**Tabulka 9.2:** Oprávnění registru a jejich významy

| Oprávnění | Význam |
|---|---|
| Úplné řízení (Full Control) | Umožní uživateli nebo skupině provést libovolné akce související s kterýmkoli jiným oprávněním. |
| Dotazovat se na hodnotu (Query Value) | Umožní dotázat se registru na hodnotu podklíče. |
| Nastavit hodnotu (Set Value) | Umožní vytvořit nové hodnoty nebo upravit existující hodnoty pod určeným klíčem. |
| Vytvořit podklíč (Create Subkey) | Umožní vytvořit nový podklíč pod určeným klíčem. |
| Vytvářet výčty podklíčů (Enumerate Subkeys) | Umožní získat seznam všech podklíčů určitého klíče. |
| Oznámit (Notify) | Umožní zaregistrovat funkci zpětného volání, která je aktivována při změně vybrané hodnoty. |
| Vytvářet propojení (Create Link) | Umožní vytvořit odkaz na určený klíč. |
| Odstranit (Delete) | Umožní odstranit klíč nebo hodnotu. |

| Oprávnění | Význam |
|---|---|
| Zapsat DAC (Write DAC) | Umožní zapsat řízení přístupu k určenému klíči. |
| Zapsat vlastníka (Write Owner) | Umožní převzít vlastnictví vybraného klíče. |
| Řízení čtení (Read Control) | Umožní přečíst volitelný seznam řízení přístupu (DACL) pro určený klíč. |




**Obrázek 9.12:** Pomocí dialogového okna Upřesnit nastavení zabezpečení lze změnit způsob dědění či nastavení oprávnění a zobrazit nastavení auditování, vlastnictví a skutečných oprávnění



## Řízení vzdáleného přístupu k registru

Hackeři a neautorizovaní uživatelé se mohou pokusit o vzdálený přístup k registru systému stejným způsobem jako oprávnění správci. Chcete-li mít jistotu, že se do registru nedostanou, můžete vzdálený přístup k registru zakázat. Vzdálený přístup k registru systému lze mj. řídit pomocí klíče registru HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg. Pokud chcete omezit vzdálený přístup k registru, můžete nejdříve změnit oprávnění k tomuto klíči.

Jestliže tento klíč existuje, projeví se změna oprávnění takto:

1. Systém Windows Server 2008 pomocí oprávnění ke klíči určí, kdo může k registru vzdáleně přistupovat. Ve výchozím nastavení mají vzdálený přístup povolen všichni ověření uživatelé. V praxi mají ověření uživatelé k tomuto klíči oprávnění Dotazovat se na hodnotu (Query Value), Vytvářet výčty podklíčů (Enumerate Subkeys), Oznámit (Notify) a Řízení čtení (Read Control).
2. Systém Windows Server 2008 pak pomocí oprávnění ke klíčům stanoví přístup k jednotlivým klíčům.

Pokud klíč neexistuje, systém Windows Server 2008 umožní vzdálený přístup k registru všem uživatelům a pomocí oprávnění ke klíčům pouze zjišťuje, ke kterým klíčům je možné přistupovat.

**DO DETAILU**

**Služby mohou vyžadovat vzdálený přístup k registru**

Některé služby potřebují ke svému správnému fungování vzdálený přístup k registru. Týká se to mimo jiné služeb Replikace adresáře (Directory Replicator) a Zařazování tisku (Spooler). Omezíte-li vzdálený přístup k registru, musíte obejít omezení přístupu pro služby. Můžete buď přidat název účtu služby do seznamu přístupu v klíči Winreg nebo uvést klíče, ke kterým služba potřebuje přístup, do hodnoty Machine nebo Users pod klíčem AllowedPaths. Obě hodnoty jsou řetězce typu REG_MULTI_SZ. Cesty, které zadáte do hodnoty Machine, umožňují přístup k uvedeným umístěním místnímu počítači (LocalSystem). Cesty zadané do hodnoty Users poskytují uživatelský přístup k uvedeným umístěním. Pokud pro tyto klíče neexistují explicitní omezení přístupu, je vzdálený přístup povolen. Po provedení změn je nutné restartovat počítač, aby bylo možné změnit konfiguraci přístupu k registru při spuštění.

Systémy Windows Vista a Windows Server 2008 ve výchozím nastavení zakazují vzdálený přístup ke všem cestám registru. Vzdáleně dostupné jsou proto pouze ty cesty registru, které jsou explicitně povoleny v rámci výchozí konfigurace nebo správcem. Vzdálený přístup k registru můžete povolit nebo zakázat pomocí zásad Možnosti zabezpečení (Security Options) v konzole Místní zásady zabezpečení (Local Security Policy). U systémů Windows Vista a Windows Server 2008 jsou pro tento účel k dispozici dvě nová nastavení zabezpečení:

- Přístup k síti: (Network Access:) Vzdáleně přístupné cesty registru (Remotely Accessible Registry Paths)
- Přístup k síti: (Network Access:) Vzdáleně přístupné cesty registru a jejich podřízené větve (Remotely Accessible Registry Paths and Sub-Paths)

Tato nastavení zabezpečení určují, ke kterým cestám a podřízeným cestám registru lze přistupovat pomocí sítě, bez ohledu na uživatele či skupiny uvedené v seznamu řízení přístupu (ACL) klíče registru Winreg. Nastaveno je několik výchozích cest, které byste neměli měnit, aniž byste pečlivě zvážili rizika, která se změnou těchto nastavení souvisejí.

Pomocí následujících kroků můžete získat přístup a upravit tato nastavení v konzole Místní zásady zabezpečení (Local Security Policy):

1. Klepněte postupně na tlačítko Start, příkaz Nástroje pro správu (Administrative Tools) a na položku Místní zásady zabezpečení (Local Security Policy). Zobrazí se konzola Místní zásady zabezpečení (Local Security Policy).
2. V levém podokně rozbalte uzel Místní zásady (Local Policies) a vyberte uzel Možnosti zabezpečení (Security Options).
3. V hlavním podokně by se měl zobrazit seznam nastavení zásad. Pomocí posuvníku přejděte v seznamu dolů na nastavení zabezpečení. Podle potřeby poklepejte na položku Přístup k síti: Vzdáleně přístupné cesty registru (Network Access: Remotely Accessible Registry Paths) nebo Přístup k síti: Vzdáleně přístupné cesty registru a jejich podřízené větve (Network Access: Remotely Accessible Registry Paths and Sub-Paths).
4. Na kartě Nastavení místní zásady (Local Policy Setting) dialogového okna vlastností (Properties) je zobrazen seznam vzdáleně přístupných cest a podřízených cest registru, který závisí na aktuálním nastavení zabezpečení. Nyní lze přidat nebo odebrat cesty či podřízené cesty podle potřeby. Výchozí nastavení jsou uvedena na kartě Vysvětlit (Explain).

**POZNÁMKA**

Systém Windows Server 2008 obsahuje službu s názvem Vzdálený registr (Remote Registry). Tato služba v praxi řídí vzdálený přístup k registru. Tuto službu je vhodné zakázat pouze v případě, že se pokoušíte před neautorizovaným přístupem chránit izolované systémy, například tehdy, je-li systém v hraniční síti a dostupný z Internetu. Pokud zakážete službu Vzdálený registr před spuštěním služby Směrování a vzdálený přístup (Routing and Remote Access), nebude možné zobrazit ani změnit nastavení konfigurace této služby. Služba Směrování a vzdálený přístup načítá a zapisuje konfigurační informace do registru. Každá akce, která vyžaduje přístup ke konfiguračním informacím, proto může zastavit činnost této služby. Chcete-li tento problém vyřešit, zastavte službu Směrování a vzdálený přístup, spusťte službu Vzdálený registr a poté restartujte službu Směrování a vzdálený přístup.

## Auditování přístupu k registru

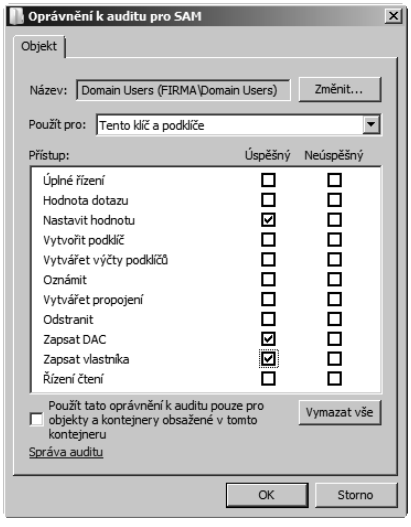
Přístup k registru lze auditovat stejně jako v případě přístupu k souborům a jiným oblastem operačního systému. Auditování umožňuje sledovat, kteří uživatelé k registru přistupují a jaké operace provádějí. Auditovat je možné všechna oprávnění uvedená v předchozí tabulce 9.1. Obvykle se však auditování omezuje na nejnutnější minimum, aby se zmenšil objem dat zapisovaných do protokolů zabezpečení a snížilo zatížení prostředků příslušného serveru.

Chcete-li povolit auditování registru, musíte nejdříve povolit funkci auditování v systému, se kterým pracujete. Můžete to provést buď pomocí místních zásad serveru nebo s použitím příslušného objektu Zásad skupiny. Auditování je řízeno zásadou Konfigurace počítače\Nastavení systému Windows\Nastavení zabezpečení\Místní zásady\Zásady auditu (Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy). Další informace o auditování a zásadách skupin naleznete v kapitolách 14 a 36.

Když povolíte auditování systému, můžete konfigurovat, jakým způsobem se auditování uplatní v případě registru. To znamená, že je nutné nakonfigurovat auditování pro každý klíč, který chcete sledovat. Díky dědičnosti naštěstí není nutné procházet všechny klíče v registru a povolovat auditování pro jednotlivé klíče. Místo toho stačí vybrat kořenový klíč nebo libovolný podklíč, abyste určili začátek větve, pro kterou chcete sledovat přístup. Poté zkontrolujte, zda se nastavení auditování dědí pro všechny podřízené podklíče (jedná se o výchozí nastavení).

Řekněme například, že chcete auditovat přístup ke klíči HKLM\SAM a jeho podklíčům. Chcete-li to provést, postupujte takto:

1. Když naleznete klíč v Editoru registru, klepněte na něj pravým tlačítkem myši a vyberte příkaz Oprávnění (Permissions). Případně vyberte klíč a klepněte na příkaz Oprávnění (Permissions) v nabídce Úpravy (Edit). Tím zobrazíte dialogové okno Oprávnění pro SAM (Permissions for SAM).
2. V dialogovém okně Oprávnění pro SAM klepněte na tlačítko Upřesnit (Advanced).
3. V dialogovém okně Upřesnit nastavení zabezpečení (Advanced Security Settings) klepněte na kartu Auditování (Auditing).
4. Po klepnutí na tlačítko Přidat (Add) vyberte uživatele nebo skupinu, jejichž přístup chcete sledovat.
5. Když vyberete uživatele či skupinu, klepněte na tlačítko OK. Zobrazí se dialogové okno Položka oprávnění pro SAM (Auditing Entry for SAM), které vidíte na obrázku 9.13.




**Obrázek 9.13:** V dialogovém okně Položka oprávnění můžete určit oprávnění, která chcete sledovat

6. Pro každé oprávnění vyberte typ auditování, které chcete sledovat. Pokud chcete sledovat úspěšné použití oprávnění, zaškrtněte sousední políčko Povolit (Successful). Chcete-li sledovat neúspěšné použití oprávnění, zaškrtněte sousední políčko Odmítnout (Failed). Zavřete dialogové okno klepnutím na tlačítko OK.
7. Opakujte krok 6, abyste nastavili auditování pro jiné uživatele nebo skupiny.
8. Jestliže chcete, aby se auditování vztahovalo na podklíče, zaškrtněte políčko Zahrnout zděditelné položky auditu z tohoto nadřazeného objektu (Include Inheritable Auditing Entries from This Object's Parent).
9. Dvakrát klepněte na tlačítko OK.