

kapitola

9

**Zavádění
a správa
softwaru
prostřednictvím
zásad skupiny**

Obsah kapitoly:

9.1 Základy instalace softwaru prostřednictvím zásad skupiny.....	328
9.2 Plánování zavádění softwaru.....	332
9.3 Zavádění softwaru prostřednictvím zásad skupiny	336
9.4 Konfigurace pokročilých a obecných možností instalace softwaru	343
9.5 Zavádění sady Microsoft Office a aktualizací	357
9.6 Správa zavedených aplikací	363
9.7 Shrnutí.....	376

Instalace a správa softwaru je náročná činnost (jak časově, tak z hlediska lidské práce) bez ohledu na to, zda pracujete na zavádění nových aplikací, implementování aktualizací nebo instalaci záplat. Mezi všemi dostupnými produkty a nástroji, které slouží k usnadnění instalace a správy software, je jen málo tak intuitivních a mocných, jako jsou zásady Software Installation. Pomocí zásad Software Installation (Instalace softwaru) můžete efektivně a centrálně spravovat celý životní cyklus svého softwaru (od jeho instalace přes opravy, záplatování, aktualizace a odstranění). Efektivní centrální správa značně snižuje náročnost zavádění a správy softwaru, což pro vaši organizaci může znamenat v konečném efektu i finanční úsporu.

Související informace

- Další informace o zavádění zásad skupiny najdete ve 4. kapitole.
- Další informace o Instalační službě systému Windows najdete na internetové adrese http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/windows_installer_start_page.asp.
- Další informace o Zavádění sady Microsoft Office 2003 pomocí zásad skupiny najdete přímo v sadě Office 2003 Resource Kit nebo na internetové adrese <http://www.microsoft.com/resources/documentation/office/2003/all/reskit/en-us/depc04.mspx>.

9.1 Základy instalace softwaru prostřednictvím zásad skupiny

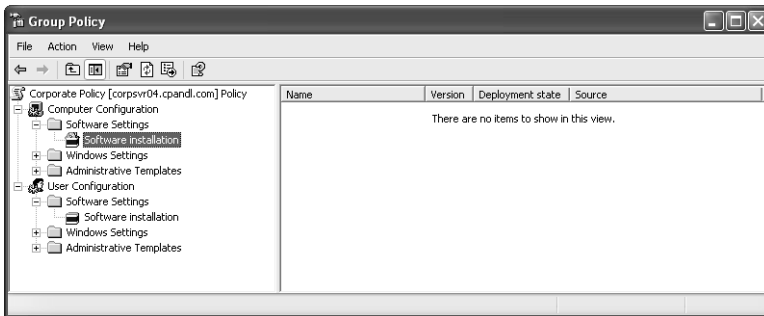
Zásady Software Installation nejsou náhradou podnikových řešení, jako je např. Microsoft Systems Management Server (SMS). jsou spíše navrženy jako univerzální a snadno použitelné řešení pro zavádění a správu softwaru v rámci oddělení. Ještě předtím, než zabředneme do samotného procesu zavádění, podíváme se na to,

- jak probíhá instalace software,
- co potřebujete vědět před instalací,
- jak nastavit zdroj instalace,
- jaká jsou omezení.

Jak probíhá instalace software

Instalace softwaru prostřednictvím zásad skupiny funguje následovně: V objektu GPO zásad skupiny pro vaši doménu služby Active Directory nadefinujete jednu nebo více aplikací. Když uživatel nebo počítač zpracuje daný objekt GPO, nainstalují se všechny aplikace, které jsou nadefinované v zásadách Software Installation tohoto objektu. Jestliže je objekt GPO připojen například k organizační jednotce Finance a vy prostřednictvím zásad Software Installation (Instalace softwaru) zavádíte Microsoft Office, nainstaluje se tento aplikační balík pro všechny uživatele a počítače organizační jednotky Finance. V celém procesu hrají roli také určité podmínky, které budou v rámci této kapitoly ještě zmíněny, ale uvedený mechanismus proces instalace v podstatě vystihuje.

Software zavedený prostřednictvím zásad skupiny je softwarem spravovaným. Zásady Software Installation se v rámci zásad skupiny nacházejí ve složkách Computer Configuration\Software Settings\Software Installation (Konfigurace počítače\Nastavení softwaru\Instalace softwaru) a User Configuration\Software Settings\Software Installation (Konfigurace uživatele\Nastavení softwaru\Instalace softwaru) (viz obrázek 9.1), což znamená, že software můžete zavádět buď pro jednotlivé počítače, nebo pro jednotlivé uživatele.



OBRÁZEK 9.1: Umístění nastavení zásad Software Installation

Obecně se dá říci, že aplikace instalované pro jednotlivé počítače jsou dostupné všem uživatelům daného počítače a aplikace instalované pro jednotlivé uživatele jsou k dispozici pouze jednotlivým uživatelům. Přístup samotných počítačů a uživatelů k aplikacím se odvíjí od toho, zda jsou připojeni na objekt GPO, který konfigurujete.

Přístupová práva k instalačnímu balíčku aplikace a souvisejících instalačních souborů mohou ovlivnit také samotné zavádění. Jestliže zavádíte software pro jednotlivé počítače, musí mít odpovídající účty počítačů přístupová práva pro čtení. Jestliže zavádíte software pro jednotlivé uživatele, musí mít práva pro čtení uživatelské účty.



Poznámka Narozdíl od většiny ostatních zásad se zásady Software Installation aplikují pouze v rámci zpracování na popředí, a nikoliv během aktualizace zásad na pozadí. Zavádění pro jednotlivé počítače probíhá během spuštění a zavádění pro jednotlivé uživatele probíhá během přihlášení.

Co potřebujete vědět před instalací

Předtím než budete moci začít zavádět svůj software, budete potřebovat instalační balíček aplikace, kterou si přejete zavést. Jak bude zmíněno v oddíle „Zavádění softwaru prostřednictvím zásad skupiny“ této kapitoly, instalační balíček obsahuje instalační soubor (balíček Instalační služby systému Windows s příponou .msi nebo aplikační balíček s příponou .zap) a aplikační soubory, které jsou potřebné pro instalaci softwaru.

Základní instalační balíček lze různě přizpůsobit. Obvykle se používají transformační soubory. Tyto soubory mají příponu .mst a používají se k úpravě instalačního procesu ve smyslu jeho optimalizace pro různé uživatele a skupiny uživatelů. Transformační soubory vám umožňují přizpůsobit téměř všechny aspekty balíčku Instalační služby systému Windows. V případě aplikací, které mají standardní instalační balíček, můžete získat nástroj pro tvorbu transformačních souborů. U většiny přizpůsobených balíčků, které si takto vytvoříte, budete ale muset při tvorbě transformačních souborů pravděpodobně spoléhat na nástroje od jiného dodavatele, než je ten, který dodává samotnou aplikaci.



Poznámka Abyste mohli plně využít výhod zásadami řízené instalace a správy, musí být instalační balíčky ověřené pomocí balíčkovacího formátu Instalační služby systému Windows. Nicméně prostřednictvím zásad Software Installation je možné zavádět také jiné balíčky než jen ty, které jsou ve formátu Instalační služby systému Windows. Háčkem ale je, že v takovém případě nebudete mít k dispozici žádné z funkcí pro správu životního cyklu aplikací. Další informace najdete v oddíle „Zavádění softwaru pomocí jiných instalačních balíčků“ této kapitoly.



Tip Transformační soubory jsou natolik obvyklým způsobem optimalizace zavádění balíčku Microsoft Office, že firma Microsoft poskytuje v sadě Microsoft Office Resource Kit nástroj s názvem Custom Installation Wizard. Více se o něm dozvíte v oddíle „Použití transformačních souborů pro optimalizaci zavádění sady Microsoft Office“ této kapitoly.

Kromě samotného instalačního balíčku potřebujete ve své síti určit také distribuční bod, aby byl balíček dostupný pro uživatele a počítače. Toto instalační umístění by se mělo nacházet ve sdílené síťové složce, která je přístupná pro všechny uživatele a počítače, na které software zavádíte. Tito uživatelé a počítače potřebují alespoň oprávnění pro čtení složky a souborového systému, na němž se balíček a související soubory nacházejí. V úvahu byste měli vzít také geografické umístění serveru, který hostí sdílenou složku (především ve vztahu k umístění uživatelů a počítačů).



Tip Umístění zdroje instalace dobře zvažte. Jakmile umístění jednou nastavíte, nebudete mít již možnost jej v objektu GPO změnit bez toho, abyste museli aplikace znovu zavést.

Při problémech s odezvou nebo kapacitou sítě se může stát, že bude potřeba umístit instalační balíčky na server nacházející se ve stejném fyzickém umístění nebo ve stejném pracovišti, jako se nacházejí uživatelé a počítače. V některých případech můžete použít systém DFS (Windows Distributed File System) a tyto soubory geograficky roz distribuovat na několik serverů. Pomocí DFS můžete vytvořit logickou adresářovou strukturu, která je nezávislá na skutečném umístění souborů v síti.

Protože systém DFS nevyjadřuje skutečné, ale virtuální umístění souborů, nebudete muset dodatečně měnit cestu k balíčku uvedenou v objektu GPO. Budete-li chtít něco změnit, uděláte to v DFS. Můžete například vytvořit kořenový adresář DFS \\AppSvr\aplikace a v něm pro jednotlivé aplikace vytvořit podadresáře. Tyto podadresáře můžete umístit na různé servery a nakonfigurovat několik fyzických spojení do stejných logických adresářů. Jestliže bude některý z těchto serverů nedostupný, postačí změnit odkaz tak, aby ukazoval na jiný server, aniž byste přitom museli zasahovat do nastavení objektu GPO.

V případě, že použijete systém DFS, který je součástí služby Active Directory, získáte několik dalších výhod:

- Možnost nakonfigurovat automatickou replikaci obsahu složky aplikace. Tato funkce vám umožňuje nakopírovat nové instalační balíčky do určité složky a následně je nechat automaticky překopírovat na ostatní servery, které tyto soubory potřebují.
- Protože systém DFS dokáže rozpoznávat jednotlivá pracoviště, budou se clientské počítače vždy připojovat ke kopii složky systému DFS, která spadá pod jejich pracoviště. To znamená, že klient se bude vždy snažit stáhnout balíček ze serveru, který je ze síťového hlediska blízko, čímž se minimalizuje doba odezvy.

Jak nastavit zdroj instalace

Umístění instalačního balíčku na sdílené místo často obnáší prosté zkopírování instalačního souboru a potřebných aplikačních souborů do zvoleného umístění, které bude zdrojem instalace. Pro některé aplikace (především aplikace firmy Microsoft) je ale lepším řešením do sdílené složky, kterou chcete použít pro zavedení balíčku, provést tzv. instalaci pro správu.



Tip Pro většinu aplikací firmy Microsoft můžete instalaci pro správu vyvolat tak, že příkazu `setup.exe` předáte parametr `/a`.

Hlavní důvod použití instalace pro správu namísto vytvoření prosté kopie instalačních souborů aplikace z distribučního disku CD-ROM je ten, že instalaci pro správu můžete v budoucnu dynamicky záplatovat a aktualizovat. Jakmile instalaci zaktualizujete, můžete pomocí funkce Redeploy aplikovat aktualizace na všechny cílové klienty (při následující aktualizaci zásad). Tím se značně zjednodušuje údržba aplikačního balíčku u klientů, které jej mají nainstalován. Druhá možnost – kopírování a provádění aktualizace mimo zásady skupiny jednotlivě pro všechny počítače – je náročná na čas i lidskou práci, proto se instalace pro správu obecně doporučuje.

Jaká jsou omezení

Přestože zásady Software Installation (Instalace softwaru) poskytují univerzální prostředky pro zavádění a správu softwaru, hodí se spíše pro zavádění softwaru na úrovni oddělení než celého podniku. Proč? Protože se na tento přístup vztahují také určitá omezení, která byste při uvažování o plošném zavádění aplikací měli vzít v potaz.

Jedním z hlavních omezení je to, že zásady lze pro distribuci softwaru použít pouze pro počítače s operačními systémy Windows 2000 či Windows XP Professional. Serverové verze operačních systémů rodiny Windows sice mohou mít Instalační

službu systému Windows, ale nemohou přijímat aplikace zaváděné prostřednictvím zásad. Počítače s operačními systémy Windows 95, Windows 98 a Windows NT Workstation také nemohou přijímat aplikace zaváděné prostřednictvím zásad. Jestliže máte ve své organizaci klientské počítače, na kterých běží některé z operačních systémů, které zavádění aplikací tímto způsobem nepodporují, budete se muset uchýlit k jinému řešení. Naskýtá se Microsoft Systems Management Server (SMS) nebo Intel LANDesk.

Dalším omezením může být způsob, kterým se zaváděné aplikace posílají po síti. U podnikových řešení jako je SMS můžete zavádění aplikace naplánovat a použít vícesměrové vysílání. Plánování vám umožňuje provést instalaci kdykoliv si přejete (například uprostřed noci, kdy není na síti žádný uživatel). Vícesměrové vysílání vám umožňuje poslat po síti jednu kopii softwaru a vyžádat si její příjem několika klienty současně. To znamená, že aplikaci můžete poslat do sítě jen jednou a nechat všechny klienty v síti, aby ji přijali.

Zásady skupiny naopak žádné plánování ani vícesměrové vysílání nepodporují. Klientské počítače zaváděnou aplikaci přijímají, když nastane určitá konfigurovatelná událost (např. zapnutí počítače, přihlášení uživatele nebo aktivace uživatele), a jinak už dobu instalace aplikace ovlivnit nemůžete. Jednotliví klienti také přijímají vlastní kopii aplikace zasílané po síti.

Další podstatné omezení souvisí s určováním, kdo má softwarový balíček obdržet. Podniková řešení, jako je SMS nebo LANDesk, mají zabudované funkce, kterými je možné vymezit, které klientské počítače (v závislosti na jejich konfiguraci) dostanou instalaci určitého softwaru. Zavádění můžete regulovat v závislosti na operačním systému, hardwaru nebo existenci předchozí verze zaváděné aplikace.

V rámci zásad skupiny je hlavním způsobem řízení distribuce aplikací přiřazení objektu GPO a filtrování. Můžete například vytvořit objekt GPO, nakonfigurovat nastavení zásad Software Installation a poté tento objekt GPO připojit k organizační jednotce Prodej. Tento objekt pak bude ovlivňovat všechny uživatele organizační jednotky Prodej. Jak bylo řečeno v oddíle „Filtrování podle bezpečnostní skupiny, uživatelé či počítače“ kapitoly 3, bezpečnostní filtr můžete použít tak, aby se objekt GPO vztahoval pouze na určité bezpečnostní skupiny v rámci pracoviště, domény nebo organizační jednotky. Vyšší stupeň kontroly můžete získat tak, že upravíte zabezpečení na samotném instalačním souboru (viz oddíl „Řízení zavádění pomocí bezpečnostní skupiny“ této kapitoly).

Vytvořit můžete také filtr služby WMI a filtrovat zavádění aplikací podle operačního systému či hardwarové konfigurace nebo podle nainstalovaných aplikací. Ačkoliv můžete s filtry služby WMI dosáhnout dobrých výsledků, mohou být někdy zrádné a před použitím je třeba je dobře otestovat. Další podrobnosti o filtrech služby WMI najdete v oddíle „Tvorba objektů GPO pro zavádění softwaru“ této kapitoly.

9.2 Plánování zavádění softwaru

Přípravu před zaváděním softwaru a nastavení zdroje instalace máme za sebou, tak se můžeme podívat na proces plánování. Pro zavádění všech druhů softwaru platí, že plánování je potřeba věnovat dostatek času. Zavádění aplikací prostřednictvím

zásad skupiny rozhodně není výjimkou. Klíčové faktory, které je potřeba zvážit, jsou následující:

- Použití speciálních objektů GPO pro zavádění softwaru
- Zda software distribuovat pro jednotlivé uživatele nebo počítače

Tvorba objektů GPO pro zavádění softwaru

V rámci plánování byste se měli zamyslet nad tím, které objekty zásad při zavádění softwaru použijete. Snadno můžete podlehnout pokušení použít existující strukturu pracoviště, domény či organizační jednotky, ale je dobré si uvědomit, že tento přístup vás do jisté míry omezuje. Pro lepší pochopení uvedeme příklad: Do organizační jednotky Prodej potřebujete zavést sadu aplikací Microsoft Office 2003. Upravíte objekt GPO organizační jednotky Prodej a nakonfigurujete zásady Software Installation. Poté zjistíte, že software potřebujete zavést i pro zbytek podniku. V tomto okamžiku můžete buď upravit objekty GPO všech zbývajících organizačních jednotek, nebo změnit způsob zavádění softwaru, což je pravděpodobně lepší volbou.

Namísto upravování objektů GPO jednotlivých pracovišť, domén a organizačních jednotek můžete vytvořit objekty GPO, které budou sloužit výhradně pro zavádění softwaru. Když pak budete potřebovat zavést software do nějakého pracoviště, domény nebo organizační jednotky, objekt GPO pro zavádění softwaru jednoduše připojíte k pracovišti, doméně nebo organizační jednotce. Obecně se doporučuje vytvořit jeden objekt GPO pro každou aplikaci nebo kategorii aplikací, kterou chcete zavádět. Jestliže potřebujete zavést například aplikaci Microsoft Visio, můžete vytvořit objekt GPO s názvem Visio Deployment Policy, nakonfigurovat jej pro zavádění programu Visio a poté objekt GPO připojit k odpovídajícím pracovištím, doménám či organizačním jednotkám vaší organizace.

Při tvorbě a konfiguraci objektu GPO určeného pro zavádění softwaru musíte vzít v úvahu i to, komu je software určen. Zásady se implicitně vztahují na všechny uživatele či počítače spadajícího do daného pracoviště, domény či organizační jednotky, ke které jste objekt GPO připojili. Toto chování ale nemusí být vždy žádoucí. Dejme tomu, že například chcete, aby všichni vývojáři měli kopii programu Visio, ale vývojáři jsou roztroušeni po celé organizaci. Přichází následující dilema: jak zavést Visio pouze pro vývojáře, aniž byste přitom museli provádět individuální instalace na počítačích všech vývojářů. Jedním způsobem, jak tento problém vyřešit, je využít strukturu bezpečnostních skupin vaší organizace pro filtrování použití zásad. Jestliže u objektu GPO pro zavádění softwaru nakonfigurujete bezpečnostní filtrování tak, aby se zásady aplikovaly pouze pro členy bezpečnostní skupiny Vývoj, zavede se program Visio pouze pro vývojáře.

Některé situace jsou ale složitější. Může se například stát, že program Visio budete chtít zavést pouze na počítače s určitou konfigurací (např. pouze pro počítače řady Dell Dimension 8300). V tomto případě (nebo kdykoliv budete chtít omezit použití zásad pouze pro určitou systémovou konfiguraci, operační systém či hardware) musíte použít filtr služby WMI. Vytvoříte filtr služby WMI, který rozpozná výrobce a model počítače, a poté filtr připojíte k objektu GPO pro zavádění softwaru tak, aby se zásady aplikovaly pouze na počítače s touto konfigurací. Filtr služby WMI by vypadal takto:

```
Root\cimV2;Select * FROM Win32_ComputerSystem WHERE Manufacturer="Dell
Computer Corporation" and Model="Dimension 8300"
```

V tomto příkladě se filtr služby WMI využije k prohledání objektu Win32_ComputerSystem a výběru všech počítačů, které mají výrobce nastaveného na hodnotu Dell Computer Corporation a model na hodnotu Dimension 8300. Předtím než takový druh filtru použijete v produkčním prostředí, nezapomeňte jej otestovat.



Tip Při použití filtrů služby WMI budete pracovat se dvěma základními objekty: Win32_ComputerSystem a Win32_OperatingSystem. Užitečný nástroj pro seznámení s těmito objekty a souvisejícími hodnotami se nazývá Netsh Diag. Při práci s nástrojem Netsh Diag nepotřebujete vědět nic o službě WMI na to, abyste pochopili, které hodnoty můžete při filtrování využít. Publikace *Microsoft Windows Command-Line Pocket Consultant* (Microsoft Press, 2004) popisuje techniky práce s nástrojem Netsh Diag a objekty Win32_ComputerSystem a Win32_OperatingSystem.

Konfigurace zavádění softwaru

Zásady Software Installation (Instalace softwaru) se aplikují pouze během zpracování zásad na popředí, a nikoliv během aktualizace zásad na pozadí. Aplikace můžete zavádět několika způsoby:

- Přiradit software ke klientským počítačům tak, aby se nainstaloval při spuštění počítače.
- Rozdistribuovat software tak, aby jej počítač mohl nainstaloval při jeho prvním použití.
- Přiradit software k uživatelům tak, aby se nainstaloval během přihlašování uživatele.
- Publikovat aplikaci tak, aby jej uživatelé mohli ručně instalovat prostřednictvím nástroje Přidat nebo odebrat programy.

Chcete-li instalaci softwaru kompletně zautomatizovat, můžete zavádění provést pomocí přiřazování. Software můžete přiřadit buď pro jednotlivé počítače, nebo pro jednotlivé uživatele. Přiřazení softwaru pro jednotlivé počítače znamená, že software se nainstaluje během příštího restartu odpovídajících počítačů. Protože se software instaluje pro jednotlivé počítače, bude k dispozici všem uživatelům, kteří se na dané počítače přihlásí.

Když aplikaci přiřadíte nějakému uživateli, je výchozí instalační režim během přihlášení daného uživatele takový, že proběhne pouze inzerce aplikace, nikoliv její plná instalace. Inzerování (instalace aplikace proběhne při prvním použití) je schopnost Instalační služby systému Windows, kterou lze využít pomocí zásad skupiny. Inzerování vám v podstatě umožní poskytnout instalaci na vyžádání, a když se použije ve spojení se zásadami Software Installation, poskytuje způsob distribuce softwaru pouze pro uživatele, kteří jej opravdu potřebují. Tento přístup může snížit nutnost údržby softwaru tam, kde to není potřeba, a správce také nemusí explicitně distribuovat aplikaci v okamžiku, kdy si uživatel vzpomene, že aplikaci konečně potřebuje začít používat.

Inzerování funguje tak, že aplikace se nenainstaluje, dokud uživatel nevyžaduje něco, k čemu je daná aplikace potřeba – ať už se jedná o dokument, nebo

o funkčnost. Abyste mohli využívat výhod inzerování, musí být Instalační služba systému Windows nastavená na poskytování aplikace prostřednictvím inzerování namísto plné místní instalace.

Aplikace může být inzerována třemi způsoby:

- **Zástupci** Balíček může nainstalovat zástupce na plochu uživatele nebo do nabídky Start. Když uživatel klepne za účelem spuštění aplikace na nějakého zástupce, nainstaluje se celá aplikace.
- **Přidružení souborů** Balíček může zaregistrovat přípony souborů a přiřadit zaváděnou aplikaci k určité souborové příponě (např. .doc pro aplikaci Word nebo .vsd pro aplikaci Visio®). Když uživatel otevře nějaký soubor s příponou spojenou s inzerovanou aplikací, tato aplikace se nainstaluje.
- **Součásti COM** Pro aplikace, které obsahují sdílené součásti COM, může balíček inzerovat tyto součásti do registru, a zajistit tak instalaci při prvním použití. Jestliže je například nainstalována aplikace Microsoft Outlook (ale aplikace Word ještě nainstalována není) a uživatel se rozhodne použít pro psaní emailů program Word, aplikace se nainstaluje v okamžiku, kdy uživatel z programu Outlook zavolá odpovídající součást.

Další možností uživatelského přiřazení je nainstalovat aplikaci po přihlášení uživatele. Přihlašovací proces ale pak kvůli instalaci aplikace zabere delší dobu.

Poslední možností zavádění je publikování aplikace a její zpřístupnění pro jednotlivé uživatele. Když aplikaci publikujete pro uživatele, dojde k jejímu inzerování při dalším přihlášení uživatele. Narozdíl od výše popsaného způsobu inzerování má tato technika svá omezení. Aplikace se inzeruje do seznamu Přidat nebo odebrat programy a současně je k dispozici k instalaci při prvním použití. To znamená, že uživatel může nainstalovat aplikaci ručně pomocí nástroje Přidat nebo odebrat programy nebo instalaci spustit pokusem o otevření souboru přidruženého k dané aplikaci.

Důkaz úspěšného inzerování uvidíte, když se podíváte na vlastnosti zástupce inzerované aplikace. Například na obrázku 9.2 byla uživateli prostřednictvím zásad přiřazena aplikace Visio 2003. V seznamu vlastností zástupce si všimněte hodnoty položky Target Type. Uvedená hodnota znamená, že když uživatel klepne na tohoto zástupce, začne instalace programu Visio.

Bez ohledu na metodu, kterou použijete, kroky vedoucí k samotnému zavedení softwaru pomocí zásad jsou v podstatě stejné. Při rozhodování, zda zavádění softwaru směřovat na počítače, nebo na uživatele, vám může pomoci tabulka 9.1, která shrnuje výhody a nevýhody přiřazování softwaru počítačům, přiřazování uživatelům a publikování.



OBŘÁZEK 9.2: Prohlížení inzerovaného zástupce programu Visio

TABULKA 9.1: Přehled metod zavádění softwaru

Oblast	Přiřazení počítači	Přiřazení uživateli	Uživatelské publikování
Aktivace	Pro instalaci softwaru je nutný restart počítače	Pro instalaci či inzerici softwaru je nutné přihlášení uživatele	Instalace softwaru nebo zahájení instalace musí být provedeno uživatelem
Dostupnost	Dostupný všem uživatelům počítače	Software je přiřazený uživateli a následuje jej všude, kam se uživatel přihlásí	Software je přiřazený uživateli při instalaci
Požadavky na uživatelskou akci	Instalace proběhne během spouštění, proto není potřebná žádná akce	Instalace proběhne během přihlášení nebo při prvním použití, proto není potřebná žádná akce	Uživatelská akce je nutná.

9.3 Zavádění softwaru prostřednictvím zásad skupiny

Zavádění softwaru prostřednictvím zásad skupiny většinou závisí na tom, kterou technologii Instalační služby systému Windows pro zavádění použijete a na správě životního cyklu. Zavést můžete ale také balíček, který nebyl připraven pomocí technologie Instalační služby systému Windows. To znamená, že existují dva základní přístupy k zavádění a správě softwaru:

- Zavádění softwaru pomocí balíčků Instalační služby systému Windows
- Zavádění softwaru pomocí jiných instalačních balíčků

Obě tyto techniky jsou popsány v následujících oddílech.

Zavádění softwaru pomocí balíčků Instalační služby systému Windows

Balíčky Instalační služby systému Windows jsou navrženy za účelem zjednodušení instalace softwaru. Technologie Microsoft Installer – Instalační služby systému Windows – je závislá na dvou základních součástech:

- Soubor instalačního balíčku softwaru
- Instalační služba softwaru

Soubor instalačního balíčku softwaru obsahuje databázi informací s podrobnostmi o tom, jak by se měl software instalovat a odstraňovat. Tento soubor má příponu `.msi` a používá jej Instalační služba systému Windows (`Msiexec.exe`). Instalační služba systému Windows je standardní komponentou na všech počítačích s operačním systémem rodiny Windows. Služba při čtení balíčkových souborů s příponou `.msi` využívá dynamicky připojovanou knihovnu `Msi.dll`.

Obsah balíčku poskytuje instalační službě informace o tom, které aplikační soubory by měly být na místní počítač zkopírovány, které zástupce vytvořit, které položky registru upravit atd. Stejně informace lze využít při rušení instalace aplikace, aby bylo dosaženo kompletního odstranění softwaru. Použití Instalační služby systému Windows má mnoho výhod, mezi které patří i možnost oprav aplikací, které byly prostřednictvím této služby nainstalovány. Jak to funguje? Balíček Instalační služby systému Windows obsahuje všechny podrobnosti potřebné k instalaci a odinstalování odpovídající aplikace. Protože balíček obsahuje seznam všech souborů a informace o systémové konfiguraci potřebné k tomu, aby software mohl správně fungovat, instalační soubor je možné použít také k opravě poškozené aplikace. Princip fungování je následující: Uvažujme, že soubor nutný pro běh aplikace byl smazán nebo poškozen. Výsledkem je, že uživateli se aplikaci nedaří spustit. Protože aplikace byla nainstalována pomocí Instalační služby systému Windows, informace v instalačním souboru lze použít při obnově poškozeného či chybějícího souboru.

Mezi další výhody zavádění softwaru pomocí Instalační služby systému Windows patří:

- **Eskalace oprávnění** Když k instalaci aplikací přiřazených nebo publikovaných pro uživatele použijete zásady, proběhne zpracování ve zvýšeném kontextu zabezpečení, aby aplikace mohli úspěšně nainstalovat i uživatelé, kteří nepatří do místní skupiny Administrators ani do skupiny Power Users. Balíček se během instalace aplikace nachází v kontextu privilegovaného uživatele s plnými právy k provádění instalací aplikací.
- **Transformační soubory** Pomocí zásad Software Installation můžete během zavádění aplikace automaticky aplikovat jeden nebo více transformačních souborů Instalační služby systému Windows. Transformační soubory vám umožňují přizpůsobit výchozí balíček Instalační služby systému Windows a upravit prvky aplikace, které se instalují na uživatelský počítač.
- **Inzerování** Tato funkce (mluví se o ní také jako o instalaci při prvním použití) je schopnost Instalační služby systému Windows, kterou lze podpořit zásadami Software Installation. Když přiřadíte nějakou aplikaci uživateli, bude během přihlášení uživatele výchozím instalačním režimem inzerování (namísto spuštění plné instalace). Inzerce jsou sady přiřazení, které mají určitý „aktivátor“. Tím

může být zástupce, přípona souboru (např. .doc pro soubory aplikace Microsoft Word) nebo registrace objektu COM. Jestliže uživatel spustí jeden z těchto aktivátorů, aplikační balíček se nainstaluje.

- **Aktualizace** Pomocí zásad Software Installation můžete mezi novými a starými verzemi aplikací nastavit aktualizací vztahy. Jestliže jste dříve pomocí zásad zavedli například sadu Microsoft Office XP, můžete zavést sadu Microsoft Office 2003 a mezi ní a předchozí verzí vytvořit aktualizací vztah. Všechny počítače a uživatelé, pro které byla dříve zavedena sada Microsoft Office XP získají po zpracování zásad Software Installation novou verzi sady (Microsoft Office 2003).
- **Automatické odstranění** Pomocí zásad Software Installation můžete automaticky odstranit (odinstalovat) aplikaci tehdy, když uživatel či počítač již nespadá do vlivu objektu GPO, které aplikaci původně nainstaloval. Jestliže se některému uživateli například nainstaluje program Microsoft Excel na základě toho, že se nachází v organizační jednotce Finance domény služby Active Directory, můžete určit, že v okamžiku, kdy změní pracovní pozici a přestěhuje se do organizační jednotky Marketing, aplikace Excel bude při dalším zpracování zásad skupiny na popředí automaticky odinstalována.

Získání potřebného souboru Instalační služby systému Windows

Časem zjistíte, že téměř každá nová aplikace má soubor balíčku s příponou .msi, který lze použít k instalaci a odinstalování aplikace. Když je součástí aplikace souborový balíček s příponou .msi, označuje se jako *nativní soubor Instalační služby systému Windows*. Použití nativní soubor Instalační služby systému Windows k zavádění softwaru pomocí zásad skupiny je nejjednodušší technikou zavádění, ale můžete si také vytvořit vlastní instalační soubor.

Jestliže chcete vytvořit soubor Instalační služby systému Windows, budete potřebovat nástroj pro jejich tvorbu (např. „WISE for Windows Installer“ od firmy Wise Solutions, Inc.). Postup, který vede k vytvoření balíčku .msi, se liší v závislosti na tom, jaký nástroj použijete, ale základní princip je následující:

1. Začnete s čistou instalací všech operačních systémů, na které chcete software zavést. Jestliže chcete software zavádět například na operační systém Windows XP Professional, spusíte na počítači novou instalaci systému Windows XP Professional. Neinstalujte žádný další aplikační software.
2. Po dokončení instalace operačního systému použijte nástroj pro tvorbu balíčků k vytvoření snímku aktuálního stavu počítače. Tento snímek musíte vytvořit před tím, než aplikaci nainstalujete.
3. Nainstalujte aplikaci na počítač. Ve většině případů stačí provést standardní instalaci softwaru. Při instalaci zvolte možnosti, které vašim uživatelům poskytnou nejlepší podporu a konfiguraci.
4. Po nainstalování aplikace zoptimalizujte konfiguraci aplikace. Můžete vytvořit nebo odstranit zástupce aplikace, přizpůsobit nástrojové lišty, nastavit výchozí možnosti atd. Aplikaci alespoň jednou spusíte pro případ, že obsahuje nějaké součásti, které se instalují až po spuštění.
5. Prostřednictvím nástroje pro tvorbu balíčků vytvořte druhý snímek systému. Během tohoto procesu vytvořte soubor Instalační služby systému Windows.

6. Uvedený postup zopakujte pro všechny operační systémy, na které máte v úmyslu software zavést. Jestliže chcete instalovat na systémy Windows 2000 i Windows XP Professional, budete obvykle potřebovat dva samostatné instalační soubory.

Jakmile máte připravené potřebné instalační soubory, můžete pomocí zásad provést distribuci softwaru ve vaší organizaci.

Zavádění softwaru pomocí souboru Instalační služby systému Windows

Až budete mít svůj soubor Instalační služby systému Windows a všechny potřebné soubory zkopírujete do sdílené síťové složky, můžete pomocí zásad skupiny nakonfigurovat instalaci softwaru. Jak bylo již řečeno v oddíle „Tvorba objektů GPO pro zavádění softwaru“, ve většině případů byste měli vytvořit nový objekt GPO, nakonfigurovat zásady Software Installation a poté objekt GPO připojit k odpovídajícím pracovištím, doménám či organizačním jednotkám, do kterých se má software zavést.

Chcete-li nakonfigurovat zásady Software Installation (Instalace softwaru) pro zavedení vašeho softwaru, postupujte takto:

1. V zásadách skupiny otevřete nastavení Software Installation. Při zavádění softwaru pro jednotlivé počítače použijte složku Computer Configuration\Software Settings\Software Installation (Konfigurace počítače\Nastavení softwaru\Instalace softwaru). Při zavádění softwaru pro jednotlivé uživatele použijte složku User Configuration\Software Settings\Software Installation (Konfigurace uživatele\Nastavení softwaru\Instalace softwaru).
2. Klepněte pravým tlačítkem na nastavení Software Installation a zvolte položku New, Package.
3. Do dialogu Open zadejte cestu k síťové sdílené složce, kde se nachází váš balíček, nebo umístění balíčku určete tak, že jej nalistujete a označíte.



Upozornění Jestliže zavádíte balíček ze síťové sdílené složky, musíte při definování balíčku v zásadách zadat cestu k této složce vždy ve standardu UNC. Proto lze obecně říci: nepoužívejte lokální cesty. Jestliže do zásad zadáte například cestu `c:\packages\office2003\pro.ms.i`, protože se balíček nachází na disku C daného serveru, bude klient zpracovávající tyto zásady hledat balíček na svém disku C.

4. Klepněte na tlačítko Open. Jestliže síťovou cestu nelze z nějakého důvodu ověřit, objeví se varovná zpráva s dotazem, zda si přejete pokračovat. Odpovíte-li Ano, použije se zadaná cesta. Odpovíte-li Ne, proces zavádění se přeruší a vy budete muset začít znovu.



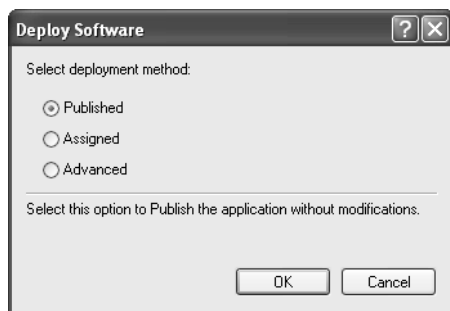
Upozornění Poté co klepnete na tlačítko Open, neexistuje již způsob, jak změnit instalační cestu softwarového balíčku. To znamená, že když vyberete špatnou cestu nebo ji potřebujete později upravit, musíte balíček smazat a vytvořit znovu.

5. V dialogu Deploy Software (Zavedení aplikace) (viz obrázek 9.3) jsou k dispozici možnosti Published, Assigned a Advanced (Publikované, Přiřazené, Upřesnit). Vyberte-li možnost Published, aplikace bude publikována bez úprav. Když vybe-

rete možnost Assigned, aplikace se přiřadí beze změn. Jestliže chcete zavést aplikaci pomocí pokročilé konfigurace, zvolte možnost Advanced (viz oddíl „Konfigurace pokročilých a obecných možností instalace softwaru“ této kapitoly).



Poznámka Obecné výchozí nastavení dokáže určit, zda se má zobrazit dialog Deploy Software. Jestliže se dialog nezobrazí, je výchozí možnost zavádění nastavena. Další informace najdete v oddíle „Nastavení výchozích možností zavádění“ této kapitoly.



OBRÁZEK 9.3: Volba metody zavádění

Jakmile jsou zásady nakonfigurovány, aplikace se odpovídajícím způsobem zavede na všechny vybrané počítače či uživatele. Softwarové balíčky pro jednotlivé počítače jsou implicitně poskytovány při spuštění počítače a softwarové balíčky pro jednotlivé uživatele jsou poskytovány během přihlášení uživatele. Jak bylo uvedeno ve 3. kapitole v oddíle „Manuální aktualizace zásad skupiny“, k vynucení restartu a odhlášení můžete použít také nástroj příkazového řádku Gpupdate.

Zavádění softwaru pomocí jiných instalačních balíčků

Chcete-li zavádět software pomocí jiných instalačních balíčků (balíčků, které nepatří Instalační službě systému Windows), musíte vytvořit speciální textový soubor označovaný jako soubor ZAP (Zero Administration Package). Jakmile budete mít potřebný soubor ZAP, můžete prostřednictvím zásad skupiny nakonfigurovat zavádění softwaru. Tento přístup má ale svá omezení a neposkytuje výhody spravované aplikace, jakými jsou např. eskalace oprávnění, správa životního cyklu a automatické odstraňování. Konkrétně můžete provádět pouze publikování pro jednotlivé uživatele, což znamená, že program se zařadí do seznamu Přidat nebo odebrat programy jako dostupná aplikace a uživatel ji odtud bude moci nainstalovat. Jestliže uvedete informace o příponách souborů přiřazených zaváděné aplikaci, dosáhnete tak také omezené možnosti instalace při prvním použití.

To je vše, co můžete dělat s instalačními balíčky, které nepatří Instalační službě systému Windows. Instalace aplikací proběhne prostřednictvím běžného instalačního souboru a s běžnými oprávněními daného uživatele. To znamená, že instalaci nemůžete upravit ani tak, že instalačnímu souboru předáte parametry. Nemůžete například provádět instalaci se zvýšenými oprávněními, proto bude uživatel pravděpodobně potřebovat oprávnění místního správce, aby aplikace mohl nainstalovat. Další věcí je, že nemáte k dispozici výhody, jako je automatické opravování, aktualizace či záplatování, které jsou dostupné v rámci Instalační služby systému Windows.



Poznámka Kvůli omezením se soubory ZAP nejlépe uplatní při zavádění aplikací, které není potřeba aktualizovat nebo záplatovat. Jediný způsob, jak aplikovat záplatu na software zavedený pomocí souborů ZAP, je pomocí zásad odstranit existující software a poté pomocí zásad znovu zavést jeho novou verzi.

Vytváření souboru formátu ZAP

Soubor ZAP je standardní inicializační soubor systému Windows s hlavičkou a sadou dvojic klíč-hodnota. Tento soubor je možné vytvořit v běžném textovém editoru (např. Poznámkový blok) a musí se uložit s příponou `.zap`, aby jej zásady Software Installation dokázaly rozpoznat.

Abby byly soubory formátu ZAP platné, musí obsahovat alespoň tyto oddíly a klíče:

```
[Application]
FriendlyName="ApplicationName"
SetupCommand="\\Servername\Sharename\Applicationinstaller.exe" /Parameter
```

Řetězec `ApplicationName` je název, který se zobrazí v seznamu Přidat nebo odebrat programy, `\\Servername\Sharename\Applicationinstall.exe` je celá síťová cesta k instalačnímu souboru aplikace a `Parameter` je parametr, který chcete instalačnímu souboru aplikace předat.

Abychom si ukázali, jak by obsah souboru vypadal pro nějakou skutečnou aplikaci, uvažujme následující příklad:

```
[Application]
FriendlyName="Microsoft Visio 2003"
SetupCommand="\\cpandl.com\dfsroot\packages\Visio 2003\setup.exe" /unattend
```

V tomto příkladě se z doménové sdílené složky `packages` spouští soubor `Setup.exe`. Při volání se mu předává přepínač `/unattend`, který spustí zavádění aplikace v bezobslužném režimu. Všimněte si, že tento přepínač není závislý na instalačním balíčku. Vaše aplikační balíčky mohou podporovat jiné přepínače, s jejichž pomocí docílíte bezobslužné instalace.



Poznámka Při nastavování instalační cesty byste měli dávat pozor na několik věcí. Jestliže cesta k souboru, který chcete spustit, obsahuje mezery nebo dlouhé názvy, musí být uzavřena v uvozovkách. Nezapomeňte ani na to, že použijete-li v hodnotě klíče `SetupCommand` písmena jednotek, zavádění aplikace se nezdaří.

Hodnoty `FriendlyName` a `SetupCommand` reprezentují minimální informace, které je potřeba uvést v souboru ZAP k tomu, aby se aplikace úspěšně zavedla. Nepovinné dvojice klíč, hodnota mohou posloužit k tomu, aby se uživatel v seznamu Přidat nebo odebrat programy zobrazil dodatečné informace. Následující klíče dokáží poskytnout dodatečné informace o aplikaci:

```
DisplayVersion = VersionNumberToDisplay
Publisher = SoftwarePublisher
URL = SoftwarePublishersURL
```

Hodnota `VersionNumberToDisplay` určuje revizní číslo softwaru, které se zobrazí v seznamu Přidat nebo odebrat programy, `SoftwarePublisher` je jméno výrobce

softwaru a SoftwarePublishersURL je URL-adresa webové stránky výrobce softwaru. Zde je příklad použití těchto klíčů:

```
DisplayVersion = 11.0
Publisher = Microsoft Corporation
URL = http://www.microsoft.com/office
```

Následující oddíl a dvojice klíč, hodnota vám zprostředkují částečnou funkcionalitu instalace při prvním použití (slouží k přiřazení souborové přípony publikované aplikaci):

```
[ext]
ext=
```

Řetězec `ext` zde vyjadřuje samotnou příponu, kterou chcete přiřadit publikované aplikaci. V následujícím příkladě se souborová přípona `.vsd` adresuje pomocí oddílu s názvem `[ext]`:

```
ext]
vsd=
```

Jestliže uživatel, pro kterého byla tato aplikace publikována prostřednictvím souboru ZAP, otevře nějaký soubor s příponou `.vsd`, aplikace se nainstaluje z cesty uvedené v klíči `SetupCommand`. Ale vzhledem k tomu, že zavádění pomocí souborů ZAP neposkytuje eskalaci oprávnění, musí mít uživatel na svém počítači dostatečná práva na to, aby instalace proběhla úspěšně.

V ukázce 9.1 je celý obsah souboru ZAP vycházející z výše uvedených příkladů.

UKÁZKA 9.1: Vzorový soubor ZAP obsahující povinné a nepovinné hodnoty

```
[Application]
FriendlyName="Microsoft Visio 2003"
SetupCommand="\\cpand1.com\dfsroot\packages\Visio 2003\setup.exe" /unattend
DisplayVersion = 11.0
Publisher = Microsoft Corporation
URL = http://www.microsoft.com/office
[ext]
vsd=
```

Zavádění softwaru pomocí souboru ZAP

Jakmile připravíte soubor ZAP a do síťové sdílené složky zkopírujete všechny potřebné soubory, můžete v zásadách skupiny nakonfigurovat instalaci softwaru. Jak bylo uvedeno v oddíle „Tvorba objektů GPO pro zavádění softwaru“, ve většině případů byste měli vytvořit nový objekt GPO, nakonfigurovat zásady Software Installation a objekt GPO poté připojit k pracovištím, doménám či organizačním jednotkám, do kterých se bude software zavádět.

Chcete-li zásady Software Installation (Instalace softwaru) nakonfigurovat pro zavedení vašeho softwaru, postupujte následovně:

1. Instalační soubory, které nespádají pod Instalační službu systému Windows, je možné instalovat pouze pro jednotlivé uživatele. Ve složce User Configura-

on\Software Settings\Software Installation (Konfigurace uživatele\Nastavení softwaru\Instalace softwaru) najdete položku Software Installation.

2. Klepněte na ni pravým tlačítkem a zvolte příkaz New, Package (Nový balíček).
3. Do dialogu Open (Otevřít) zadejte cestu k síťové sdílené složce, ve které se nachází váš balíček, nebo balíček nalistujte a vyberte.



Upozornění Jestliže zavádíte balíček ze síťové sdílené složky, musíte při definování balíčku v zásadách vždy zadat cestu k balíčku ve formátu UNC. Stručně řečeno, nepoužívejte místní cesty. Jestliže do zásad zadáte například cestu `c:\packages\visio\viso.zap`, protože balíček se nachází na disku C daného serveru, bude klient zpracovávající tyto zásady hledat balíček na svém disku C.

4. V seznamu Files of Type (Typy souborů) vyberte jako typ souboru možnost ZAW Down-Level Applications Packages (*.zap).
5. Klepněte na tlačítko Open. Jestliže se z nějakého důvodu nepodaří ověřit síťovou cestu, objeví se varovná zpráva s dotazem, zda si přejete pokračovat. Odpovíte-li Ano, použije se zadaná cesta. Odpovíte-li Ne, proces zavádění se přerušuje a vy budete muset začít znovu.



Upozornění Poté co klepnete na tlačítko Open, neexistuje již způsob, jak cestu k souboru ZAP změnit. To znamená, že když vyberete špatnou cestu nebo ji potřebujete později upravit, musíte balíček vytvořit znovu.

6. Vyberete-li v dialogu Deploy Software možnost Published (Zavedení aplikace – Publikované), aplikace bude publikována bez úprav. Jestliže chcete zavést aplikaci pomocí pokročilé konfigurace, zvolte možnost Advanced (viz následující oddíl).



Poznámka Obecné výchozí nastavení dokáže určit, zda se má zobrazit dialog Deploy Software. Jestliže se dialog nezobrazí, je výchozí možnost zavádění nastavena. Další informace najdete v oddíle „Nastavení výchozích možností zavádění“ této kapitoly.

Jakmile je objekt GPO nakonfigurován, aplikace se může odpovídajícím způsobem inzerovat na všechny vybrané počítače či uživatele. Zásady Software Installation se pro uživatele implicitně publikují pouze během jejich přihlašování. Jak bylo uvedeno ve 3. kapitole v oddíle „Manuální aktualizace zásad skupiny“, k vynucení odhlášení můžete použít také nástroj příkazového řádku Gpupdate.

9.4 Konfigurace pokročilých a obecných možností instalace softwaru

Poté co vytvoříte přiřazený nebo publikovaný softwarový balíček, můžete pomocí možností pokročilé instalace softwaru upravit jeho vlastnosti. Tyto možnosti jsou dostupné, také když v dialogu Deploy Software zvolíte jako druh balíčku možnost Advanced. Tyto možnosti můžete použít k:

- prohlížení a nastavování obecných možností zavádění,
- změně druhu zavádění a instalačních možností,

- definování kategorií aplikací pro jejich snazší správu v případě, že zavádíte větší množství aplikací,
- označení balíčku jako aktualizace dříve zavedené aplikace,
- definování transformačních souborů, které chcete použít pro přizpůsobení instalace,
- řízení zavádění pomocí bezpečnostní skupiny.

Dalšími možnostmi jsou obecné možnosti instalace softwaru, které můžete použít k nastavení obecných možností zásad Software Installation.

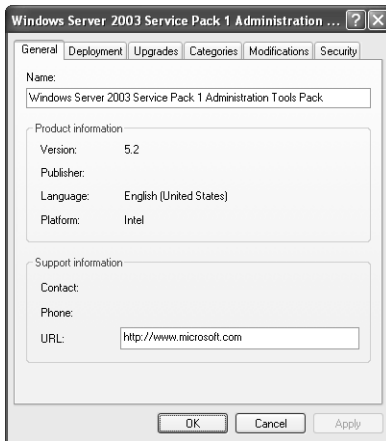
Prohlížení a nastavování obecných možností zavádění

Obecné možnosti zavádění softwarového balíčku slouží především pouze pro informační účely a patří mezi ně:

- **Name (Název)** Název, pod kterým bude balíček uveden v seznamu Přidat nebo odebrat programy. Tento název je určen vlastností `ProductName` uvedenou v souboru s příponou `.msi` nebo vlastností `FriendlyName` ze souboru ZAP. Název je možné změnit prostřednictvím obecných možností.
- **Product Information (Informace o produktu)** Podrobnosti o verzi, vydavateli, jazyce a platformě zjištěné z balíčku. V souboru ZAP se verze a vydavatel specifikují prostřednictvím vlastností `DisplayVersion` a `Publisher`. Když jsou jednou informace o produktu nastaveny, nelze je již později změnit.
- **Support Information (Uživatelská podpora)** Jméno kontaktní osoby, telefonní číslo a URL-adresa výrobce softwaru. V souboru ZAP se URL-adresa udává pomocí vlastnosti `URL`. Adresu URL je možné změnit prostřednictvím obecných možností.

Obecné možnosti softwarového balíčku můžete prohlížet a upravovat následujícím způsobem:

1. Podle toho, s jakým druhem balíčku chcete pracovat, vstupte buď do složky `Computer Configuration\Software Settings\Software Installation` (Konfigurace počítače\Nastavení softwaru\Instalace softwaru), nebo do složky `User Configuration\Software Settings\Software Installation` (Konfigurace uživatele\Nastavení softwaru\Instalace softwaru) a otevřete položku `Software Installation`.
2. V pravém podokně by se měl zobrazit seznam definovaných balíčků. Pravým tlačítkem klepněte na balíček, se kterým chcete pracovat, a zvolte `Properties` (Vlastnosti).
3. Na kartě `General` (Obecné) se nacházejí informace o názvu, produktu a odborné pomoci (viz obrázek 9.4).



OBRÁZEK 9.4: Prohlížení a nastavování obecných možností softwarového balíčku

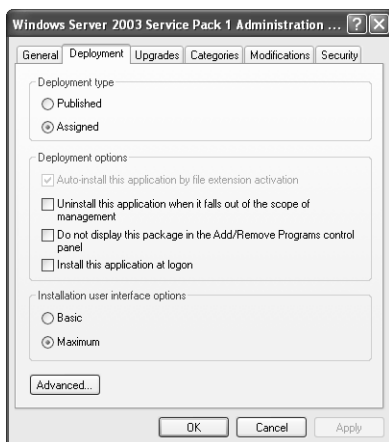
Změna druhu zavádění a instalačních možností

Během tvorby balíčku můžete nastavit pouze základní možnosti, které určují, zda se má aplikace publikovat, nebo přiřadit. Protože konfiguraci bude často potřeba ještě doladovat, měli byste v dialogu Properties vždy zkontrolovat druh zavádění a instalační možnosti a případně provést potřebné změny. Celý postup je následující:

1. Podle toho, s jakým druhem balíčku chcete pracovat, vstupte buď do složky Computer Configuration\Software Settings\Software Installation, nebo do složky User Configuration\Software Settings\Software Installation a otevřete položku Software Installation.
2. Pravým tlačítkem klepněte na balíček, se kterým chcete pracovat, a zvolte Properties. Přejděte na kartu Deployment (viz obrázek 9.5).
3. Na kartě Deployment (Zavedení aplikace) můžete vybrat, zda se aplikace má publikovat, nebo přiřadit. Podle této volby se zpřístupní, nebo zablokují další související možnosti. K dispozici jsou následující možnosti:
 - **Auto-Install This Application By File Extension Activation (Automaticky nainstalovat aplikaci při použití souboru tohoto typu)** Proveďte se inzerování souborových přípon přiřazených k balíčku, aby se aplikace zavedla při prvním použití. Tato možnost je vybrána implicitně a nelze ji změnit v případě, že balíček přiřadíte uživateli. U publikované aplikace, která obvykle vyžaduje, aby ji uživatel nainstaloval ze seznamu Přidat nebo odebrat programy, získáte zapnutím této možnosti funkce související s přiřazením souborové přípony dané aplikaci.
 - **Uninstall This Application When It Falls Out Of The Scope Of Management (Odinstalovat aplikace, jsou-li mimo obor správy)** Jestliže již uživatel nemá na aplikaci nárok, dojde k jejímu odstranění. Uživatel či počítač ztratí na aplikaci nárok v případě, že již nadále nespadá pod objekt GPO, který aplikaci zaváděl. Jestliže k uvedenému dojde a je zapnuta tato možnost, aplikace se během dalšího aktualizacího cyklu na popředí (přihlášení uživatele nebo restart počítače) odinstaluje.



Poznámka Aplikace se může stát pro uživatele či počítač nedostupnou ze tří hlavních důvodů: objekt reprezentující uživatele či počítač se v rámci hierarchie služby Active Directory přesune na jiné místo, které již nespadá do vlivu původního objektu GPO; objekt GPO je v dané správní oblasti zablokován nebo odstraněn; bezpečnostní filtrování objektu GPO se změní takovým způsobem, že uživatel či počítač již nemůže daný objekt zpracovávat.



OBRÁZEK 9.5: Prohlížení a upravování druhu zavádění a instalačních možností

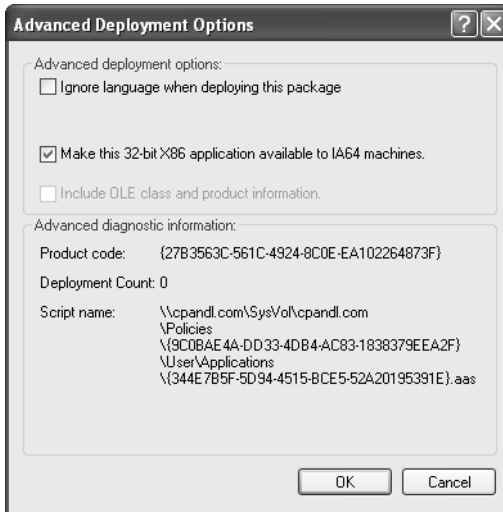
- **Do Not Display This Package In The Add/Remove Programs Control Panel (Nezobrazovat balíček v ovládacím panelu Přidat nebo odebrat programy)** Zabrání aplikaci v tom, aby se objevila v seznamu Přidat nebo odebrat programy. Tato možnost může být užitečná, když se rozhodnete uživateli se správčovskými oprávněními pro jeho počítač zabránit v tom, aby ručně odstranil aplikaci zavedenou prostřednictvím zásad.
- **Install This Application At Logon (Tuto aplikaci nainstalovat při přihlášení)** Nakonfiguruje zavádění tak, aby se po přihlášení uživatele provedla namísto inzerování plná instalace. Tato možnost je implicitně vypnutá a v případě, že publikujete balíček pro uživatele, ji nelze měnit.



Poznámka U rozsáhlých aplikací může instalace během přihlašování značně zpomalit proces přihlašování uživatele. Předtím než se uživatel dostane na plochu, musí totiž instalační program aplikace skončit.

4. Nastavení Installation User Interface Options (Možnosti uživatelského rozhraní instalace) vám umožňují nadefinovat, zda se budou uživateli během instalace aplikace zobrazovat všechny zprávy. S výchozím nastavením Maximum uvidí uživatel všechny instalační obrazovky a zprávy. S možností Basic uvidí uživatel pouze zprávy o chybách a dokončení instalace. V případě, že instalaci spustí uživatel, vyžadují některé aplikace použití možnosti Basic, neboť uživatel nemá dostatečná práva na to, aby během instalace odpovídal na dotazy instalačního programu.

5. Klepnete-li na tlačítko Advanced (Upřesnit), zobrazí se dialog Advanced Deployment Options (Upřesnit možnosti zavedení) (viz obrázek 9.6), který obsahuje následující možnosti:



OBRAZEK 9.6: Konfigurace pokročilých možností zavádění softwaru

- **Ignore Language When Deploying This Package (Při zavádění balíčku nebrat ohled na jazyk)** Tato možnost se využije, když má uživatel nainstalovanou jednu jazykovou verzi operačního systému Windows a pokouší se nainstalovat jinou jazykovou verzi nějaké aplikace. Za normálních okolností by došlo k chybě, ale když použijete tuto možnost, aplikace se nainstaluje.
- **Make This 32-Bit X86 Application Available To IA64 Machines (Zpřístupnit tuto 32bitovou verzi X86 aplikace pro počítače architektury Win64)** Tato volba vám umožní zavést 32bitové aplikace kompatibilní s procesory řady X86 na 64bitové verze operačních systémů rodiny Windows používající architekturu čipu IA-64. Tato možnost se vztahuje na aplikace nainstalované pomocí instalačních souborů .msi nebo .zap.
- **Include OLE Class And Product Information (Zahrnout třídu OLE a informace o produktu)** Umožňuje vám zahrnout do služby Active Directory registrační informace architektury COM. Jestliže zvolíte tuto možnost, inzerce architektury COM, které jsou součástí aplikačního balíčku, se umístí do úložiště Active Directory Class Store, které je součástí kontejneru GPC souvisejícího se zásadami Software Installation. Vzhledem k tomu, že velký balíček může obsahovat značné množství inzerovaných součástí COM, zvolte tuto možnost pouze v případě, že inzerování architektury COM potřebujete při svém zavádění nutně použít. Další informace o úložišti Class Store najdete ve 12. kapitole.

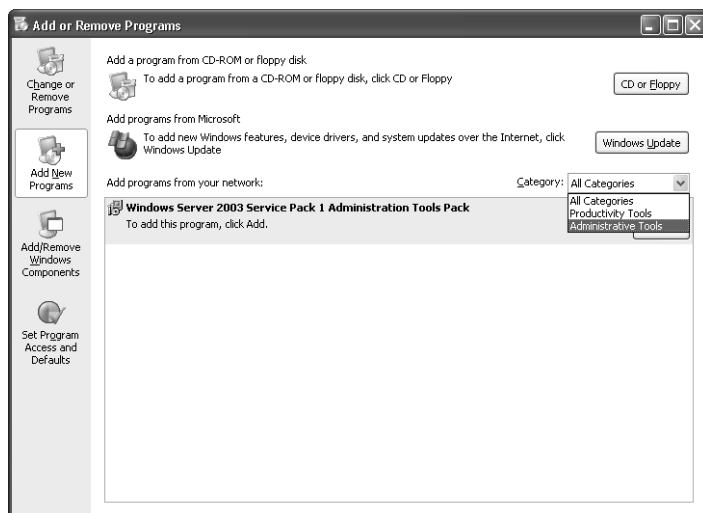


Tip Dialog Advanced Software Deployment Options obsahuje také některé užitečné diagnostické informace o balíčku. První uvedená hodnota je produktový kód Instalační služby systému Windows, který zásady Software Installation používají jako klíč k určení, zda daná aplikace již byla nainstalována na nějaký počítač. Další hodnota je počet zavádění, která udává, kolikrát se zavádění dané aplikace opakovalo. Poslední informací je cesta k přiřazovacímu skriptu aplikace. Tento soubor je uložen v objektu GPO (v části pro šablony GPT) a obsahuje informace související s cestou k balíčku a provedeným inzerováním.

Definování kategorií aplikací

Když ve velkých podnicích použijete pro zavádění velkého množství aplikací zásady Software Installation, může být žádoucí nadefinovat kategorie, které vám pomohou uspořádat seznam aplikací dostupných v seznamu Přidat nebo odebrat programy. Jestliže máte nainstalované desítky aplikací a nevytvoříte kategorie pro jejich zařazení, uživatelům se zobrazí celý seznam všech aplikací, což může být značně nepřehledné. Abyste se této situaci vyhnuli, měli byste nadefinovat kategorie aplikací (např. Prodej, Návrh, Marketing, Správa a Obecné).

Až kategorie vytvoříte, zobrazí se v dialogu Přidat nebo odebrat programy (viz obrázek 9.7). Tvorba a definování kategorií je poměrně jednoduchý proces. Nejdříve kategorie pomocí výchozích možností zavádění nadefinujete (více viz oddíl „Nastavení výchozích možností zavádění“). Poté aplikace přidáte do jednotlivých kategorií prostřednictvím možností karty Categories v odpovídajícím dialogu Properties.



OBRAZEK 9.7: Zobrazení kategorií aplikací v okně Přidat nebo odebrat programy

Přidávání, úprava a odstraňování kategorií aplikací

Kategorie aplikací se definují pomocí obecných možností zásad Software Installation. Chcete-li definovat kategorie aplikací, postupujte následovně:

1. Přejděte do složky Software Installation v Computer Configuration\Software Settings\Software Installation.

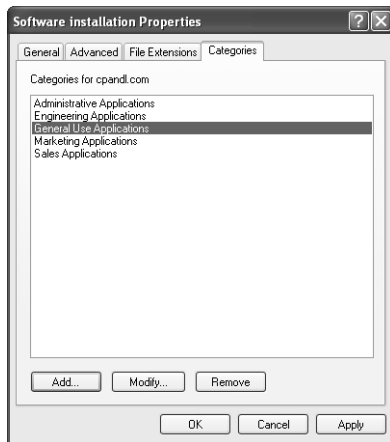


Poznámka Pro kategorie aplikací se používají stejné obecné výchozí možnosti jako pro oboje zásady Software Installation (zásady pro jednotlivé počítače i pro jednotlivé uživatele).

2. Klepněte pravým tlačítkem na položku Software Installation a zvolte Properties.
3. V dialogu Software Installation Properties přejděte na kartu Categories (viz obrázek 9.8).
4. Chcete-li nadefinovat novou kategorii aplikací, klepněte na tlačítko Add, zadejte název kategorie a poté klepněte na tlačítko OK.

Chcete-li změnit existující kategorii, vyberte ji a poté klepněte na tlačítko Modify. Poté co název kategorie změníte, klepněte na tlačítko OK.

Chcete-li existující kategorii odstranit, vyberte ji a pak klepněte na tlačítko Remove.



OBRAZEK 9.8: Tvorba a správa kategorií aplikací

Přiřazení aplikace do kategorie

Jakmile požadované kategorie nadefinujete, můžete do nich začít přidávat aplikace. Jestliže chcete přidat aplikaci do nějaké kategorie, postupujte takto:

1. Podle druhu balíčku, se kterým chcete pracovat, nalistujte složku Computer Configuration\Software Settings\Software Installation (Konfigurace počítače\Nastavení softwaru\Instalace softwaru) nebo User Configuration\Software Settings\Software Installation (Konfigurace uživatele\Nastavení softwaru\Instalace softwaru) a otevřete nastavení Software Installation.
2. Pravým tlačítkem klepněte na balíček a zvolte položku Properties (Vlastnosti). Přejděte na kartu Categories (Kategorie).
3. V seznamu Available Categories (Dostupné kategorie) vyberte požadovanou kategorii a poté klepněte na tlačítko Select (Vybrat). Jestliže si přejete, aby byla aplikace zařazena do několika kategorií, zopakujte postup popsany v tomto bodě.
4. Klepněte na tlačítko OK.

Provádění aktualizací

Jak již bylo uvedeno dříve, v případě, že použijete balíčky Instalační služby systému Windows, poskytnou zásady Software Installation aplikacím aktualizací cesty. Existují dva hlavní druhy aktualizací:

- Aktualizace, které mají provést záplatování nebo instalaci opravného balíčku.
- Aktualizace, které zavádějí novou verzi aplikace.

Následující oddíly se věnují oběma těmto druhům aktualizací. Pamatujte si, že případné aktualizace byste měli vždy pečlivě otestovat předtím, než je nasadíte do produkčního prostředí. Měli byste se ujistit, že aktualizace nezpůsobí konflikty s existujícími aplikacemi nebo jiné problémy. Také byste měli otestovat proces aktualizace a ujistit se, že funguje podle očekávání. Jestliže testování vynecháte, může se například stát, že narazíte na problémy s kompatibilitou nebo zjistíte, že jste do aktualizace nezahrnuli všechny potřebné soubory.

Instalace opravy Service Pack a záplatování

Chcete-li nějakou aplikaci záplatovat nebo na ni aplikovat opravu Service Pack, postupujte následovně:

1. Připravte si soubor `.msi` nebo `.msp` (záplata) pro danou aplikaci. Měli byste jej získat od výrobce softwaru. Jestliže jej nedostanete, musíte si vytvořit svůj vlastní (viz oddíl „Získání potřebného souboru Instalační služby systému Windows“ této kapitoly).
2. Soubor s příponou `.msi` nebo `.msp` (a případně i další potřebné instalační soubory) zkopírujte do složky s původním souborem `.msi`. Případné duplicitní soubory přepište.
3. Podle druhu balíčku, se kterým chcete pracovat, otevřete ve složce Computer Configuration\Software Settings\Software Installation nebo User Configuration\Software Settings\Software Installation položku Software Installation.
4. Znovu zaveďte aplikace. Klepněte pravým tlačítkem na odpovídající balíček a poté zvolte All Tasks, Redeploy Application (Všechny úlohy, Znovu zavést aplikaci).

Aplikace se odpovídajícím způsobem znovu zavede pro všechny uživatele a počítače spadající pod daný objekt GPO. Další informace o tom, jak opakované zavádění funguje, najdete v oddíle „Znovuzavádění aplikací“ této kapitoly. Pamatujte si, že tímto způsobem lze aktualizovat pouze aplikace, které mají soubory Instalační služby systému Windows. Jestliže vaše aplikace používá soubory ZAP, musíte postupovat následovně:

1. Odstraňte (odinstalujte) existující aplikaci (viz oddíl „Odstraňování zavedených aplikací“ této kapitoly).
2. Vytvořte pro aplikaci nový balíček (viz oddíl „Vytváření souboru formátu ZAP“ této kapitoly).
3. Zaveďte nový balíček (viz oddíl „Zavádění softwaru pomocí souboru ZAP“ této kapitoly).

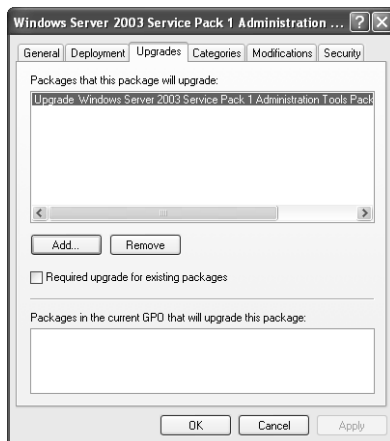
Zavádění nové verze aplikace

V dialogu Properties instalačního balíčku můžete vytvořit nebo ověřit aktualizaci vazby mezi aplikací, kterou zavádíte, a dříve zavedenými aplikacemi. Tato funkce vám umožňuje provádět vynucené aktualizace dříve nainstalovaných aplikací. Jestliže jste dříve publikovali například sadu Microsoft Office XP, můžete zavést Microsoft Office 2003 a vytvořit aktualizaci vazbu mezi instalací sady Microsoft Office XP a instalací Microsoft Office 2003. Případní uživatelé nebo počítače s aplikací Microsoft Office XP během příštího zpracování zásad na popředí automaticky získají instalaci Microsoft Office 2003.



Poznámka Když v rámci jednoho objektu GPO zavádíte dvě aplikace, které mají v produktovém kódu Instalační služby systému Windows stejná čísla SKU (třetí a čtvrtá číslice produktového kódu), aplikace zaváděná jako druhá je zavedena automaticky s aktualizací vazbou na první aplikaci. Jestliže zavedete například sadu Microsoft Office XP a poté Microsoft Office 2003, zavede se Microsoft Office 2003 automaticky jako aktualizace produktu Microsoft Office XP. Chcete-li aktualizovat dříve zavedenou aplikaci na novou verzi, postupujte následovně:

1. Vytvořte nový softwarový balíček, s jehož pomocí zavedete novou verzi aplikace (viz oddíl „Zavádění softwaru pomocí balíčků Instalační služby systému Windows“ této kapitoly).
2. Podle druhu balíčku, se kterým chcete pracovat, otevřete ve složce Computer Configuration\Software Settings\Software Installation nebo User Configuration\Software Settings\Software Installation položku Software Installation.
3. Klepněte pravým tlačítkem na odpovídající balíček a poté zvolte Properties. Jestliže je balíček již nakonfigurován k aktualizaci existujícího balíčku, bude uveden v seznamu Packages That This Package Will Upgrade (Balíčky inovované tímto balíčkem) (viz obrázek 9.9). Zvolte balíček a klepnutím na tlačítko Remove (Odebrat) odstraníte vazbu.



OBRAZEK 9.9: Konfigurace aktualizacích vazeb

4. Chcete-li mezi zaváděnou a existující aplikací vytvořit vazbu, klepněte v kartě Upgrades (Inovace) na tlačítko Add (Přidat). Otevře se dialog Add Upgrade Package (Přidat inovační balíček) (obrázek 9.10).

5. Aktualizační vztah mezi aplikacemi zaváděnými v rámci stejného objektu GPO můžete vytvořit tak, že zvolíte možnost Current Group Policy Object. Když chcete vytvořit vztah s balíčkem z jiného objektu GPO, zvolte možnost A Specific GPO, klepněte na tlačítko Browse (Procházet) a poté pomocí dialogu Browse For A Group Policy Object (Vyhledat objekt zásad skupiny) vyberte odpovídající objekt GPO.



OBRÁZEK 9.10: Přidání balíčku k aktualizaci

6. V seznamu Package To Upgrade (Balíček určený k inovaci) vyberte balíček, který se má aktualizovat. Poté můžete zvolit způsob aktualizace:
 - **Uninstall The Existing Package, Then Install The Upgrade Package (Odinstalovat stávající balíček a poté nainstalovat inovaci)** Doporučuje se v případě, že chcete aplikaci zcela přeinstalovat novou verzí.
 - **Package Can Upgrade Over The Existing Package (Balíček může být použit k inovaci přes stávající balíček)** Doporučuje se v případě, že chcete provést aktualizaci nad existující instalací.
7. Klepnutím na tlačítko OK zavřete dialog Add Upgrade Package (Přidat inovační balíček).
8. Jestliže chcete, aby aktualizace byla označena jako vyžadovaná, zaškrtněte políčko Required Upgrade For Existing Packages (Vyžadovat inovaci existujících balíčků). Aplikace, kterou zavádíte po následujícím restartu počítače nebo přihlášení uživatele, automaticky zaktualizuje existující balíčky. Uživatel nebude mít na proces žádný vliv. Jestliže aktualizaci neoznačíte jako vyžadovanou, bude mít uživatel možnost pomocí seznamu **Add/Remove Programs (Přidat nebo odebrat programy)** nebo aktivováním aplikace určit, kdy se má aktualizace nainstalovat.

Poté co vytvoříte aktualizační vazbu, balíček provádějící aktualizaci bude mít u ikony zelenou, nahoru směřující šipku, ukazující, že se jedná o aktualizaci.



Poznámka Jestliže zavádíte dvě aplikace a jedna aktualizuje druhou, pak se novým síťovým klientům, kteří nemají nainstalovanou ani jednu z nich, nainstaluje nejdříve starší verze aplikace a poté se během následujícího procesního cyklu na popředí nainstaluje aktualizovaná verze.

Přizpůsobení instalačního balíčku pomocí transformačních souborů

Když aplikace používá balíček Instalační služby systému Windows, můžete instalaci přizpůsobit pomocí transformačních souborů. Transformační soubory jsou speciální instrukční soubory, které během instalace aplikace upravují instrukce zabudované ve výchozím balíčku. Transformační soubory mají příponu `.msi`.

Transformační soubory přiřazené aplikaci můžete spravovat pomocí dialogu Properties odpovídajícího softwarového balíčku. Podle toho, s jakým druhem balíčku chcete pracovat, vstupte buď do složky Computer Configuration\Software Settings\Software Installation, nebo User Configuration\Software Settings\Software Installation a otevřete položku Software Installation. Klepněte pravým tlačítkem na odpovídající balíček, zvolte položku Properties a poté přejděte do karty Modifications (Změny).

Aplikaci můžete přiřadit několik transformačních souborů. Soubory se zpracují v pořadí uvedením na kartě Modifications (shora dolů), což znamená, že transformační soubory položené v seznamu níže mají přednost před těmi umístěnými výše. Další informace o tvorbě transformačních souborů pro balíček Microsoft Office najdete v oddíle „Zavádění sady Microsoft Office a aktualizací“ této kapitoly.



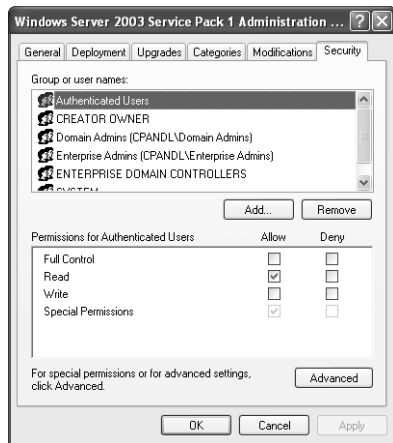
Upozornění Poté co transformační soubory přidáte k nějaké publikované nebo přiřazené aplikaci a klepnutím na tlačítko OK aplikaci zavedete, nebudete již moci seznam transformačních souborů této aplikace měnit. Chcete-li změnit použité transformační soubory, musíte aktuální aplikaci z objektu GPO odstranit, počkat, až si ji všichni odpovídající klienti odinstalují, a poté balíček v objektu GPO znovu vytvořit a zadat nové transformační soubory.

Řízení zavádění pomocí bezpečnostní skupiny

Jak již bylo řečeno dříve, množinu počítačů a uživatelů, kteří si zaváděný software nainstalují, můžete ovlivnit několika způsoby: Můžete použít bezpečnostní filtr, což způsobí, že se objekt GPO použije pouze pro určité bezpečnostní skupiny konkrétního pracoviště, domény nebo organizační jednotky. Můžete také vytvořit filtr služby WMI a filtrovat zavádění aplikace v závislosti na operačním systému či hardwarové konfiguraci. Dále můžete upravit zabezpečení na samotném instalačním souboru, což je přístup rozebíraný v tomto oddíle.

Změna zabezpečení na instalačním souboru nabízí více granulární způsob řízení toho, kteří uživatelé a počítače budou zpracovávat nastavení zásad Software Installation, než když použijete bezpečnostní filtrování založené na objektech GPO. Ačkoliv může být objekt GPO napojen na nějakou organizační jednotku a mít bezpečnostní filtrování, které určuje, že jej aplikují všichni uživatelé daného objektu GPO, můžete použít kartu Security pro řízení toho, kteří uživatelé dané organizační jednotky obdrží určitý zaváděný aplikační balíček. Protože v rámci jednoho objektu GPO můžete zavádět několik různých aplikací, stává se zavádění aplikací flexibilnějším.

Pro správu zabezpečení instalačního souboru, a tedy i správu toho, které počítače a uživatelé jej mohou využívat, se používá dialog Properties daného softwarového balíčku. Podle toho, s jakým druhem balíčku chcete pracovat, vstupte buď do složky Computer Configuration\Software Settings\Software Installation (Konfigurace počítače\Nastavení softwaru\Instalace softwaru), nebo User Configuration\Software Settings\Software Installation (Konfigurace uživatele\Nastavení softwaru\Instalace softwaru) a otevřete položku Software Installation. Klepněte pravým tlačítkem na odpovídající balíček, zvolte Properties a poté přejděte na kartu Security (Zabezpečení) (viz obrázek 9.11).



OBRAZEK 9.11: Prohlížení bezpečnostních oprávnění aplikačního balíčku

Možnosti na kartě Security vám umožňují definovat delegování pro vybraný instalační soubor v rámci objektu GPO. Výchozí zabezpečení nabízí:

- Oprávnění pro čtení uživatelům skupiny Authenticated Users, což všem uživatelům a počítačům spadajícím pod daný objekt GPO umožňuje práci se souborem.
- Oprávnění pro čtení, zápis a speciální oprávnění pro tvůrce souboru a skupinu Enterprise Admins, což tvůrci a uživatelům skupiny Enterprise Admins umožňuje pracovat s instalačním souborem.
- Oprávnění pro čtení a speciální oprávnění pro členy skupiny Enterprise Domain Controllers, což členům této skupiny umožňuje pracovat s instalačním souborem.
- Úplné řízení pro skupiny System a Domain Admins, což operačnímu systému a členům skupiny Domain Admins umožní spravovat instalační soubor a instalační proces.

Jestliže chcete uživateli či počítači (nebo skupině uživatelů či počítačů) umožnit instalaci zaváděného aplikačního balíčku, stačí jim jednoduše poskytnout práva pro čtení aplikace. Zaváděný aplikační balíček implicitně poskytuje skupině Authenticated Users práva pro čtení. Z toho vyplývá, že všichni uživatelé a počítače mají k aplikačnímu balíčku implicitně přístup. Jestliže chcete aplikační balíček zavést jen pro určitou skupinu, musíte z aplikace nejdříve odstranit oprávnění skupiny Authenticated Users a pro odpovídající uživatele, počítače a skupiny poté přidat práva

pro čtení. Nicméně protože oprávnění se dědí ze samotného objektu aplikačního balíčku, musíte před změnou oprávnění odstranit dědičnost. Tuto operaci provedete následovně:

1. Podle toho, s jakým druhem balíčku chcete pracovat, vstupte, buď do složky Computer Configuration\Software Settings\Software Installation, nebo User Configuration\Software Settings\Software Installation a otevřete položku Software Installation.
2. Klepněte pravým tlačítkem na odpovídající balíček a poté zvolte Properties. Na kartě Security klepněte na tlačítko Advanced.
3. Zrušte zaškrtnutí pole s nápisem Inherit From Parent The Permission Entries That Apply To Child Objects (Povolit přenesení dědičných oprávnění z nadřazeného objektu).
4. Otevře se dialog s dotazem, zda chcete zděděná oprávnění kopírovat či odstranit nebo zcela zrušit celou operaci. Zvolte Copy (Kopírovat). Klepněte na tlačítko OK a vrátíte se zpět do základního dialogu zabezpečení.
5. V seznamu Group Or User Names vyberte skupinu Authenticated Users a poté klepněte na tlačítko Remove.
6. Klepněte na tlačítko Add a poté v dialogu Select Users, Computers, Or Groups vyberte uživatele, počítač nebo skupinu, pro kterou chcete přidat oprávnění. Klepněte na tlačítko OK.
7. V seznamu Group Or Users Names označte nově přidaného uživatele, počítač či skupinu. V části Permissions for (Oprávnění pro) zaškrtněte ve sloupci Allow (Povolit) políčko Read (Číst).
8. Kroky 6 a 7 zopakujte pro ostatní uživatele, počítače a skupiny.
9. Klepněte na tlačítko OK.

Nově přidaní uživatelé, počítače a skupiny mohou nyní aplikaci nainstalovat. Ostatní uživatelé, počítače a skupiny aplikaci instalovat naopak nemohou (pokud nejsou členy jedné z výchozích skupin – např. Domain Admins).

Nastavení výchozích možností zavádění

Jestliže pro zásady Software Installation používáte pokaždé určité instalační možnosti, můžete využít funkce globálních výchozích možností. Jestliže například chcete, aby se aplikace automaticky odinstalovaly v případě, že na ně cílový subjekt ztratí nárok, můžete využít právě obecných výchozích možností.

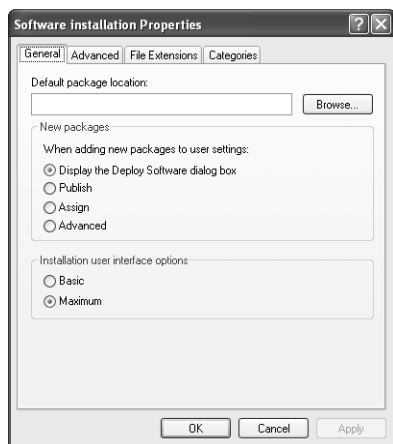
Poznámka Co se týče kategorií Software Installation Categories, používají se pro ně stejné obecné výchozí možnosti uložené v objektu GPO, bez ohledu na to, zda se jedná o instalaci pro jednotlivé počítače, nebo pro jednotlivé uživatele. Odděleně lze obecné výchozí možnosti nastavit pro zásady Software Installation v částech Computer Configuration a User Configuration.

Obecné výchozí možnosti můžete prohlížet a definovat následujícím způsobem:

1. Ve složce Computer Configuration\Software Settings\Software Installation otevřete nastavení Software Installation.

2. Klepněte pravým tlačítkem na odpovídající balíček a poté zvolte Properties. Otevře se dialog Software Installation Properties (viz obrázek 9.12).

Obecné výchozí možnosti zásad Software Installation můžete prohlížet a nastavovat jak pro uživatele, tak i pro počítače.



OBRÁZEK 9.12: Dialog Software Installation Properties

Tabulka 9.2 obsahuje přehled obecných výchozích možností, které můžete konfigurovat, a také obsahuje název karty, v níž jednotlivé možnosti najdete.

TABULKA 9.2: Obecné výchozí možnosti zásad Software Installation

Karta	Možnost	Popis
General	Default Package Location	Určuje výchozí cestu pro balíčky daného objektu GPO. Když zvolíte New, Package, objeví se tato cesta v dialogu Open File.
	New Packages	Určuje, zda se způsob zavádění vybere automaticky nebo se objeví dialog Deploy Software. Implicitně máte možnost vybrat způsob zavádění prostřednictvím dialogu Deploy Software. Můžete určit, že objekt GPO bude automaticky používat jednu z těchto možností.
	Installation User Interface Options	Určuje výchozí rozhraní: k dispozici je možnost Basic a Maximum. S výchozím nastavením, kterým je Maximum, jsou uživatelé zobrazeny všechny instalační obrazovky a zprávy. Použijete-li možnost Basic, uvidí uživatelé pouze chybové zprávy a zprávy o dokončení instalace.
Advanced	Uninstall The Applications When They Fall Out Of The Scope Of Management	Uživatel či počítač ztratí na aplikaci nárok v případě, že objekt GPO, který ji zaváděl, na uživatele či počítač již nemá vliv. Jestliže uživatel či počítač ztratí nárok na aplikaci a je vybrána tato možnost, aplikace se během příštího aktualizacího cyklu (přihlášení uživatele nebo restartování počítače) na popředí odinstaluje.

Karta	Možnost	Popis
	Include OLE Information When Deploying Applications	Jestliže zvolíte tuto možnost, inzerování architektury COM spadající do aplikačního balíčku je uloženo v úložišti Active Directory Class Store. Další informace o úložišti Class Store najdete ve 13. kapitole.
	Make 32-Bit X86 Windows Installer Applications Available To IA64 Machines	Umožňuje vám používat soubory s příponou .msi k zavádění 32bitových aplikací kompatibilních s procesory řady x86 na 64bitových verzích operačních systémů rodiny Windows používajících architekturu čipu Intel IA-64.
	Make 32-Bit X86 Down – Level Applications Available To IA64 Machines	Umožňuje vám používat soubory s příponou .zap k zavádění 32bitových aplikací kompatibilních s procesory řady x86 na 64bitových verzích operačních systémů rodiny Windows používajících architekturu čipu Intel IA-64.
File Extensions	Application Precedence	Jestliže máte v objektu GPO několik aplikací, ke kterým je přiřazena stejná souborová přípona, můžete použít tuto možnost pro řízení toho, která aplikace je nainstaluje, až uživatel otevře dokument s inzerovanou příponou.
Categories	Categories For The Domain	Umožňuje vám určit obecné výchozí možnosti pro kategorie aplikací. Kategorie se poté objeví v okně Přidat nebo odebrat programy.

9.5 Zavádění sady Microsoft Office a aktualizací

Zásady Software Installation jsou použitelné pro různé scénáře zavádění aplikací, ale nejčastěji se používají pro zavádění balíčku Microsoft Office a aktualizací operačního systému. V tomto oddíle se budeme věnovat doporučením pro oba tyto případy a také hlediskům jejich návrhu a zavádění.

Zavádění sady Microsoft Office prostřednictvím zásad

Sada Microsoft Office je pravděpodobně softwarem nejčastěji zaváděným prostřednictvím zásad. Protože jsou distribuční soubory značně objemné (500 MB a více), je Microsoft Office dobrou ukázkou toho, co je třeba zvážit při zavádění objemných aplikací prostřednictvím zásad. Při zavádění Microsoft Office nebo jakékoliv jiné rozsáhlé aplikace byste měli před zaváděním zvážit několik věcí, včetně těchto:

- Jaký způsob distribuce balíčku použijete
- Zda k přizpůsobení instalace použijete transformační soubory
- Jaký použít režim zavádění

- Jak se bude Microsoft Office aktualizovat



Poznámka Microsoft Office je po instalaci často potřeba přizpůsobit. Sada Office 2003 Resource Kit obsahuje šablony pro správu, které můžete použít pro přizpůsobení konfigurací Microsoft Office. Tomuto tématu se podrobně věnuje 10. kapitola.

Výběr způsobu distribuce balíčku

Prvním hlediskem je umístění balíčku. V podstatě máte dvě možnosti, jak dostat balíček ke klientovi: správčovská a nesprávčovská instalace.

Správčovskou instalaci sady Microsoft Office do sdílené síťové složky můžete provést pomocí přepínače `setup /a`. Jak již bylo uvedeno dříve, pro zavádění všech aplikací v zásadách byste měli používat cestu ve formátu DFS, neboť po zavedení aplikací již není možné změnit její cestu. Výhodou správčovské instalace je to, že můžete záplatovat přímo instalaci a pak provést opětovné zavedení, čímž všechny klienty donutíte, aby si aplikaci znovu nainstalovali v nové, opravené verzi.

Nesprávčovskou instalaci Microsoft Office můžete provést do síťové sdílené složky. To spočívá v tom, že obsah instalačního CD jednoduše zkopírujete do síťové sdílené složky a v zásadách se na balíček Instalační služby systému Windows odkážete. Výhodou tohoto přístupu je to, že když zavádíte sadu Microsoft Office 2003, můžete použít funkci Local Install Source pro uložení instalačních souborů Microsoft Office do mezipaměti na místní pracovní stanici. Nevýhodou nesprávčovské instalace je skutečnost, že když Microsoft Office potřebujete opravit nebo aktualizovat, musíte opravu distribuovat a spustit na všech počítačích, kde je aplikace nainstalována.



Poznámka Jestliže provádíte správčovskou instalaci produktu Microsoft Office 2003, můžete použít novou funkci Local Install Source. Tato funkce vám umožňuje uložit do mezipaměti lokálního počítače (do skryté složky MSOCache) všechny soubory s příponou `.cab` potřebné pro opravy, aktualizace nebo záplatování. Uživatel pak během aktualizací nebude potřebovat instalační CD. Prostřednictvím transformačního souboru na instalačním balíčku máte možnost určit, zda chcete, aby se na pracovní stanici během instalace Microsoft Office 2003 vytvářela mezipaměť LIS (Local Install Source). Samozřejmě je potřeba počítat s tím, že uložení všech datových souborů s příponou `.cab` do mezipaměti zabere na pracovní stanici téměř 200 MB diskového prostoru. K tomu ještě připočtete vytížení sítě spojené s kopírováním těchto souborů.

Tyto dvě možnosti se hodí nejlépe pro zavádění sady Microsoft Office na počítače s rychlým síťovým připojením k serverům, kde se nacházejí balíčky. V některých případech se ale může stát, že máte klienty, kteří jsou připojeni přes pomalou nebo dokonce vytáčenou linku. Jestliže zásady skupiny zjistí pomalé připojení, zásady Software Installation se implicitně nezpracují. A to ani během zpracování zásad na popředí. Ale i v případě, že by ke zpracování na pomalém připojení došlo, by instalace (při velikosti, jaké dosahuje Microsoft Office) trvala věčnost.

Ale i na rychlých sítích by při současném stahování 600 MB dat potřebných pro instalaci Microsoft Office pravděpodobně došlo k zahlcení sítě, což by vedlo ke značným problémům. Proto existuje třetí přístup k zavádění sady Microsoft Office nebo jakékoliv jiné rozsáhlé aplikace. Spočívá v nasazení instalačního balíčku lo-

kálně na všechny počítače před zaváděním aplikace prostřednictvím zásad. Takové řešení má dvě výhody:

- Při distribuci balíčků na počítače před zaváděním nejste časově omezováni.
- Uživatelé připojující se vzdáleně si mohou balíček stáhnout, až budou v kanceláři, nebo jim můžete zaslat CD, ze kterého si soubory zkopírují na místní počítač.

Soubory můžete klientovi doručit různými způsoby. Můžete použít cokoli od zaslání CD poštou nebo zkopírování souborů na klienty pomocí příkazu `xcopy` až po vytvoření plánovaných úloh nebo skriptů při spuštění, které se postarají o zkopírování souborů ze serveru v době, která bude pro klienta nejvíce příhodná. Použití můžete i robustnější kopírovací nástroj, jakým je např. Robocopy (součást sady Windows Server 2003 Resource Kit).

Největší překážkou při doručování souborů na klientské počítače je skutečnost, že pro rozsáhlé balíčky, jako je Microsoft Office, může být kopírování instalačních souborů extrémně náročné na kapacitu sítě. V takových případech byste měli začít uvažovat o použití síťové technologie, jako je např. vícesměrové vysílání IP, neboť tak můžete značně snížit opakované zasílání dat, která tečou vaší síťovou infrastrukturou do vzdálených sítí. Dalším řešením pro vzdálené síť je umístit instalační soubory na server ve vzdálené síti a poté vytvořit skript při spuštění (nebo jiný mechanismus), který tyto soubory stáhne ze serveru na klienty. Tímto způsobem rozložíte zátěž spojenou se zaváděním balíčku a zajistíte, že kopírování souborů proběhne pouze v rámci místních sítí (LAN).

Jakmile budete mít balíček zavedený na všechny počítače, které jej mají instalovat, můžete nastavit zásady tak, aby se odkazovaly na místní cestu, do které jste na všech počítačích nakopírovali instalační soubory. V tomto případě nepoužijete cestu ke sdílené složce UNC, ale absolutní cestu ke složce na pevném disku místního počítače (např. `c:\packages\office2003\pro11.msi`).



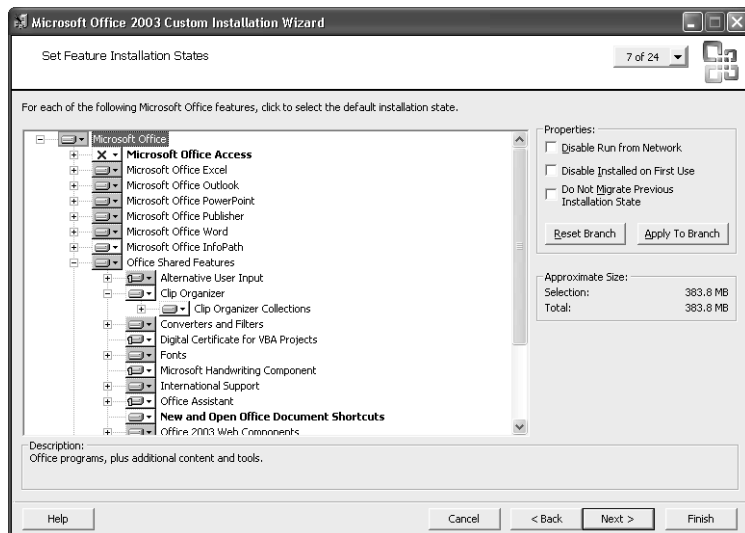
Tip Někdy se může stát, že ačkoliv na vzdálené klienty zkopírujete instalační soubory, počítače na pomalém připojení nebudou stále schopny software nainstalovat. Toto může být důsledkem toho, že funkce pro detekci pomalého připojení nebere v úvahu umístění balíčku, ale pouze skutečnost, že je počítač připojen na pomalé lince. Chcete-li se tomuto problému vyhnout a zajistit, že se zásady Software Installation vždy zpracují, zapněte na všech počítačích, kterým budete distribuovat aplikace, nastavení Allow Processing Across A Slow Network Connection nacházející se ve složce Computer Configuration\Administrative Templates\System\Group Policy\Software Installation Policy Processing. Zapnutím těchto zásad zajistíte, že počítače, na které jste nakopírovali instalační balíček, vždy provedou instalaci. A to i v případě, že jsou připojeny pomalým připojením.

Použití transformačních souborů pro optimalizaci zavádění sady Microsoft Office

Transformační soubory jsou běžnou metodou přizpůsobování instalací sady Microsoft Office. Transformační soubory vám dávají možnost upravit téměř všechny oblasti zavádění balíčku Instalační služby systému Windows. U sady Microsoft Office můžete transformační soubory použít například pro řízení toho, které aplikace sady Microsoft Office se nainstalují, jaké bude výchozí umístění dokumentů pro jednotlivé aplikace a nastavení výchozího profilu aplikace Microsoft Outlook.

Jestliže chcete vytvořit transformační soubory pro Microsoft Office 2003, musíte si stáhnout volně dostupnou sadu nástrojů Office 2003 Editions Resource Kit Tools (z internetové adresy <http://www.microsoft.com/downloads/details.aspx?FamilyID=4bb7cb10-a6e5.4334.8925.3bcf308cfbaf&DisplayLang=en>).

Po nainstalování nástrojů na vaši správcovskou stanici můžete spustit průvodce Custom Installation Wizard a vytvořit transformační soubory. Obrázek 9.13 ukazuje, jak můžete nastavit, aby některé aplikace (v tomto případě Microsoft Access) nebyly nainstalovány, zatímco jiné (např. New And Open Office Document Shortcuts), které nejsou součástí výchozí instalace, se stanou její součástí.



OBRAZEK 9.13: Průvodce Custom Installation Wizard

Když dokončíte práci s průvodcem, nástroj se vás zeptá, kam se má transformační soubor s příponou .mst uložit. Jestliže jste během přípravy zavádění instalační soubory sady Microsoft Office zkopírovali do síťové sdílené složky, umístěte kopii transformačního souboru do této sdílené složky. Jestliže máte v úmyslu zkopírovat instalační soubory na všechny počítače, měli byste transformační soubor zkopírovat spolu s instalačními soubory, abyste zajistili, že bude během instalace dostupný. Dále je potřeba nakonfigurovat zásady tak, aby se používaly transformační soubory. Podrobnosti najdete v oddíle „Přízpusobenění instalačního balíčku pomocí transformačních souborů“ této kapitoly.

Výběr režimu zavádění

Zásady Software Installation nabízejí několik způsobů zavádění aplikací (včetně přiřazování a publikování uživatelům), ale upřednostňovanou metodou zavádění rozsáhlých aplikací, jako je Microsoft Office, je přiřazování počítačům. Přiřazování počítačům je řešení, jak provést bezobslužnou instalaci, která nevyžaduje interakci ze strany uživatele. Všechny uživatelské mechanismy požadují, aby byl uživatel na pracovní stanici zablokován, dokud instalace aplikace neskončí. U aplikací, jako je

Microsoft Office, by to ale mohlo znamenat desítky minut v případě, že je síť zaneprázdněná nebo v nejlepší případě „jen“ 5 až 10 minut.

Vzhledem k tomu, že přiřazování počítačům se spouští při restartování, máte jistotu, že na počítači v době zavádění není přihlášen žádný uživatel. Jedinou komplikací přiřazování počítačům je to, že pro zahájení instalace musíte vyvolat restart počítače. Toho lze dosáhnout několika způsoby. Například použitím vzdáleného skriptu služby WMI nebo pomocí nástroje Shutdown.exe spolu s využitím Plánovače úloh.

Jestliže pro instalační soubory sady Microsoft Office používáte síťovou sdílenou složku, měli byste restartování počítačů správně rozložit, aby nedošlo k zahlcením sítě velkým počtem současných požadavků na soubory umístěné ve sdílené složce.

Aktualizování sady Microsoft Office

Když firma Microsoft vydá novou opravu nebo záplatu pro sadu Office, měli byste ji znovu zavést prostřednictvím zásad. Jestliže jste pro zavedení sady Microsoft Office použili správčovskou instalaci, je proces zavádění aktualizací poměrně jednoduchý. První věcí, kterou byste si měli zapamatovat, je, že jestliže se jedná o aktualizací balíček Service Pack, měli byste stáhnout plnou verzi (nikoliv klientskou verzi). Následně byste měli soubory aktualizace vyextrahovat do pracovního adresáře. Tento krok se týká i záplat. Soubory aktualizací balíčku či záplaty vždy nejprve rozbalte do pracovní složky namísto toho, abyste jej spouštěli přímo z vaší správčovské stanice. Pro tyto účely slouží parametry /t a /c (viz níže):

```
officexpSp3-kb832671-fullfile-enu.exe /t:C:\downloads\officexp-sp3 /c
```

Časem zjistíte, že velká část stahovaných souborů má příponu .msp. Tuto příponu používají k záplatování soubory Instalační služby systému Windows, které je potřeba aplikovat na vaši správčovskou instalaci. Jestliže chcete aplikovat aktualizace na vaši správčovskou instalaci, použijte pro záplatování hlavního souboru s příponou .msi (nacházejícího se ve sdílené složce vaší správčovské instalace) zabudovaný nástroj příkazového řádku Msiexec.exe. Příkaz pro použití záplaty je následující:

```
msiexec /p PathToMSPIFile /a PathToMSIFile SHORTFILENAME=TRUE /qb /L*  
PathToLogFile
```

Pro použití příkazu musíte znát cestu k souboru .msp, cestu k hlavnímu souboru .msi sady Microsoft Office ve vaší správčovské sdílené složce (u sady Office Professional je název obvykle pro *.msi) a cestu k souboru protokolu, který zaznamenává selhání a úspěchy procesu záplatování.

Až dokončíte záplatování všech správčovských instalačních míst, budete muset sadu Microsoft Office znovu zavést pomocí zásad. Během následujícího cyklu zpracování na popředí provedou tyto počítače/uživatelé opětovnou instalaci aktualizované verze sady Office.

Jestliže jste instalační soubory sady Office zaváděli na počítače přímo, bude proces aplikování aktualizace odlišný:

1. Zkopírujte instalační soubory aktualizací balíčku nebo záplaty na místní počítač.
2. Na všech odpovídajících klientech spusťte příkaz msiexec.exe a provede se aktualizace jejich místních instalačních zdrojů.

3. Aby se znovu spustila instalace z aktualizovaného místního zdroje, zaveďte Microsoft Office znovu do zásad.



Poznámka Jestliže používáte funkci Local Install Source sady Microsoft Office 2003, není potřeba zmiňovanou manuální operaci s příkazem *msiexec* provádět. Prostě jen na místním počítači spustíte klientskou verzi záplaty nebo aktualizacího balíčku a mezipaměť Local Install Source se zaktualizuje.

Zavádění aktualizací systému Windows prostřednictvím zásad

Další obvyklá situace je zavádění aktualizací systému Windows prostřednictvím zásad. Instalace aktualizací systému Windows se do jisté míry podobá produktu Microsoft Office, protože aktualizace Service Pack jsou obvykle poměrně velké. Nicméně s aktualizacemi systému přichází také jedno nové nebezpečí, neboť selhání uprostřed instalace aktualizacího balíčku může znamenat, že počítač se již znovu nepodaří spustit. Z toho důvodu mají aktualizací balíčky specifické požadavky.

Měli byste se vyvarovat instalování aktualizací ze správčovské sdílené složky. Zhoršená odezva a výpadky sítě by mohly mít nepříjemné důsledky. Obzvláště v případě, že by k nim došlo uprostřed aktualizace. Jestliže máte v síti nějaké vzdálené počítače, které by v okamžiku selhání neměly k dispozici žádné fyzické systémové prostředky pro správu, je lepší na ně nakopírovat soubory aktualizacího balíčku před provedením aktualizace.

Pro zavádění aktualizacího balíčku prostřednictvím zásad se používá stejný postup:

1. Ze stránek firmy Microsoft stáhněte plný aktualizací balíček. Mezi staženými soubory je soubor s názvem `Update.msi`, který je hlavním aktualizací souborem Instalační služby systému Windows dané aktualizace.
2. Soubor `Update.msi` použijte při definování vašeho softwarového balíčku. Stejně jako u sady Microsoft Office musíte tento balíček vytvořit tak, aby byl přiřazen počítači, čímž se zajistí, že balíček se zavede při restartu počítače bez přítomnosti uživatelů.



Tip Softwarový balíček pro aktualizaci systému Windows je nejlepší vytvořit v rámci samostatného objektu GPO. To vám umožní objekt GPO snadno připojit k libovolnému kontejneru, na který chcete aktualizaci Service Pack aplikovat.

3. Poté co vytvoříte přiřazení počítači, bude aktualizace aplikována na všechny počítače, které během následujícího restartu zpracují dané zásady. Před tím než se objeví přihlašovací dialog, dojde ještě k jednomu restartování. Budete-li chtít ověřit, že oprava byla aplikována správně, spusťte na cílové pracovní stanici příkaz `winver`.



Tip Většinou platí, že když byla aktualizace na počítač prostřednictvím zásad aplikována již dříve, její aplikace se nebude opakovat. Nicméně chcete-li si být sto procentně jisti, že k opětovné aktualizaci nedojde, můžete vytvořit filtr služby WMI, který bude před zpracováním zásad kontrolovat verzi aktualizace, a připojit jej k odpovídajícímu objektu GPO.

9.6 Správa zavedených aplikací

Zásady Software Installation jsou navrženy pro správu celého životního cyklu zaváděných aplikací. Poté co aplikace prostřednictvím zásad Software Installation zavedete, budete s největší pravděpodobností aplikaci chtít dále upravovat a později možná odstranit. Klepnete-li v objektu GPO pravým tlačítkem na zavedenou aplikaci, zobrazí se vám několik možností správy aplikace. Prostřednictvím položky v nabídce můžete například přepnout aplikaci zavedenou pro uživatele z publikované na přiřazenou. Jestliže jste dříve zvolili, že se má aplikace automaticky nainstalovat prostřednictvím aktivace přes souborovou příponu, můžete to zde pomoci změny nastavení možnosti Auto-Install vypnout.

V oddíle „Konfigurace pokročilých a obecných možností instalace softwaru“ jsme se zabývali prováděním aktualizací, přizpůsobováním instalačních balíčků pomocí transformačních souborů a dalšími úlohami rutinní údržby, které mohou být prováděny pomocí instalačních možností. Mezi dodatečné úlohy, které můžete také potřebovat, patří:

- Odstranění zavedených aplikací
- Opětovné zavedené aplikací
- Konfigurace zásad Software Restriction
- Řešení problémů

Odstraňování zavedených aplikací

Zásady Software Installation (Instalace softwaru) můžete použít pro instalování aplikací a odstraňování dříve zavedených aplikací. Proces odinstalování můžete spustit ručně odstraněním softwarového balíčku, který aplikaci v zásadách zaváděl. Odinstalování lze také vyvolat automaticky. Automatické odinstalování proběhne v případě, že cílové počítače/uživatelé ztratí na aplikaci nárok a současně je aktivní nastavení Uninstall This Application When It Falls Out Of The Scope Of Management.

Chcete-li vyvolat odstraňování dříve zavedené aplikace, postupujte takto:

1. Podle toho, s jakým druhem balíčku chcete pracovat, vstupte buď do složky Computer Configuration\Software Settings\Software Installation (Konfigurace počítače\Nastavení softwaru\Instalace softwaru), nebo User Configuration\Software Settings\Software Installation a otevřete položku Software Installation.
2. Klepněte pravým tlačítkem na odpovídající balíček a v nabídce zvolte All Tasks, Remove.
3. V dialogu Remove Software (Odebrat software) jsou k dispozici dvě možnosti odstraňování:
 - **Immediately Uninstall The Software From Users And Computers (Okamžitě odinstalovat aplikaci z počítačů a profilů uživatelů)** Okamžitě odstraní aplikaci ze všech klientů, kteří ji používají.
 - **Allow Users To Continue To Use The Software, But Prevent New Installations (Povolit uživatelům dále používat aplikaci, zabránit však no-**

vým instalacím) Zabrání dalším instalacím, ale ponechá aplikaci na počítačích, kde je již nainstalována.



Poznámka Jestliže zvolíte okamžité odstranění, nedojde k odinstalování okamžitě, ale během následujícího cyklu zpracování zásad na popředí.

4. Klepněte na tlačítko OK.



Tip Když odstraníte nějakou aplikaci, zůstává nadále v kontejneru GPC (Group Policy Container) služby Active Directory a v šabloně GPT (Group Policy Template) složky SYSVOL (přestože již není v zásadách vidět), dokud ji z nich ručně neodstraníte. Aby bylo zaznamenáno, že je balíček odstraněn, změní se hodnota atributu `msiScriptName` na objektu `package-Registration` služby Active Directory na hodnotu R. Další informace o uložení nastavení zásad najdete ve 13. kapitole.

Opětovné zavádění aplikací

Jak již bylo uvedeno v oddíle „Instalace opravy Service Pack a záplatování“, existuje několik důvodů, proč je potřeba aplikaci znovu zavádět. Jestliže záplatujete správcovskou instalaci aplikace, která byla dříve zavedena, můžete funkci opětovného zavádění využít k opětovné instalaci aktualizované aplikace pro všechny cílové uživatele a počítače. Při opětovném zavádění se aplikace přeinstaluje všude tam, kde byla dříve nainstalována. Instalace proběhne při následujícím cyklu zpracování zásad na popředí. Reinstalace spočívá v tom, že uživatelé a počítače provedou opravu zavoláním Instalační služby systému Windows s parametry `o`, `m`, `u`, `s` a `v`. Tyto parametry vyvolají následující chování:

- Jestliže chybí nějaký soubor nebo je ve starší verzi, aplikace se přeinstaluje.
- Dojde k přepsání záznamů registru (všech určených pro počítač) souvisejících s balíčkem.
- Dojde k přepsání záznamů registru (všech určených pro uživatele) souvisejících s balíčkem.
- Přepíše se všechny zástupci související s balíčkem.
- Z balíčku Instalační služby systému Windows se spustí oprava a soubor s příponou `.msi` se uloží do místní mezipaměti. (Soubory Instalační služby systému Windows s příponou `.msi` se během instalace ukládají vždy do mezipaměti lokálního počítače a jsou uloženy ve složce `%windir%\installer`.)



Poznámka Když dojde k opětovnému zavedení balíčku, všechna uživatelská nastavení a data, která byla vytvořena od první instalace aplikace, by měla být zachována. Nicméně záleží to na to na instalačním programu a na tom, kde jsou nastavení a data uložena. U aplikací, jako je Microsoft Office, jsou nastavení a data při opětovném zavádění zachována.

Konfigurace zásad Software Restriction Policies

Poté co váš software zavedete, můžete zajistit, aby se na uživatelských systémech spouštěl pouze správný software a správné softwarové verze. K tomu slouží zásady Software Restriction Policies. Tyto zásady se nacházejí v oblastech Computer Con-

figuration a User Configuration složky Windows Settings\Security Settings\Software Restrictions Policies.



Poznámka V místním objektu GPO jsou zásady Software Restriction Policy k dispozici pouze pro počítače, nikoliv pro jednotlivé uživatele.

Zásady Software Restriction Policies poskytují mocný mechanismus pro blokování spouštění softwaru. Omezovat můžete známé druhy softwaru, které působí ve vaší síti problémy (např. hry, aplikace pro sdílení dat) nebo neznámé druhy softwaru, který by mohl provádět nebezpečné aktivity.

Začínáme se zásadami Software Restriction Policies

Zásady Software Restriction Policies (Zásady omezení softwaru) se konfiguruje v objektech GPO. Zásady Software Restriction Policies nacházející se v části Computer Configuration se používají k nastavování omezení pro všechny uživatele určitého počítače. Zásady Software Restriction Policies nacházející se v části User Configuration se používají k nastavování omezení pro jednotlivé uživatele nebo skupiny uživatelů.

Když větev zásad Software Restriction Policies jedné ze zmiňovaných částí otevřete v objektu GPO poprvé, zobrazí se zpráva oznamující, že nejsou definovány žádné zásady pro omezování práce se softwarem. Práci se zásadami Software Restriction Policies zahájíte klepnutím pravým tlačítkem na větev Software Restriction Policies a zvolením položky Create New Policies (Nové zásady omezení softwaru). V podokně se zobrazí větve:

- **Enforcement policy (Vynucení)** Určuje, jak se aplikuje omezení softwaru na softwarové soubory a pro koho bude platit.
- **Designated File Types policy (Určené typy souborů)** Určuje, které typy souborů a přípony se budou považovat za spustitelné.
- **Trusted Publishers policy (Důvěryhodný vydavatel)** Nastavuje důvěryhodné distributory softwaru.
- **Security Levels node (Úroveň zabezpečení)** Obsahuje zásady, které určují, zda a jak bude spouštěn omezený software.
- **Additional Rules node (Další pravidla)** Obsahuje zásady, které řídí spouštění softwaru. Pravidla řízení lze vytvořit na základě vydavatelských certifikátů, internetové zóny (z níž software pochází), souborové cesty nebo bezpečné šifry souboru.

Dohromady vám tyto zásady umožňují nastavit obecná chování pro softwarová omezení nebo vlastní pravidla a chování pro omezení nebo povolení spouštění určitého softwaru. Jakmile tato nastavení použijete pro nadefinování pravidel svých zásad Software Restriction Policies, můžete je zavést pro vaše uživatele a počítače.

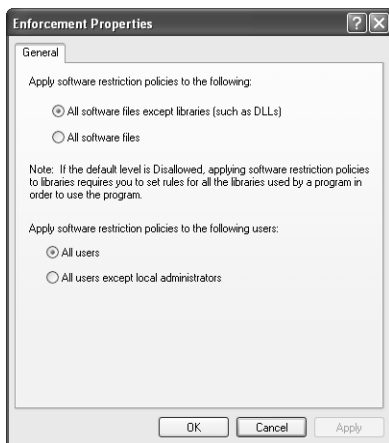
Zavedete-li zásady Software Restriction Policies pro jednotlivé počítače, nebo pro jednotlivé uživatele, závisí na tom, zda potřebujete spouštění softwaru řídit pro všechny uživatele počítače, nebo jen pro některé, bez ohledu na to, kde jsou přihlášení. Jestliže potřebujete různé úrovně řízení založené na umístění uživatele ne-

bo počítače ve službě Active Directory, můžete zásady Software Restriction Policies sloučit z několika objektů GPO.

Konfigurování zásad Enforcement

Nastavení zásad Enforcement určuje, jak se softwarové omezení použije na softwarové soubory a na koho se omezení aplikují. Chcete-li prohlížet nebo nastavovat nastavení zásad pro vynucování, postupujte takto:

1. Podle potřeby nalistujte složku Computer Configuration\Windows Settings\Security Settings\Software Restrictions Policies nebo User Configuration\Windows Settings\Security Settings\Software Restrictions Policies a otevřete položku Software Restriction Policies.
2. Jestliže nejsou softwarová omezení zatím nastavena, klepněte pravým tlačítkem na uzel Software Restriction Policies a zvolte příkaz Create New Policies.
3. V pravém podokně klepněte pravým tlačítkem na položku Enforcement a zvolte Properties.
4. Zásady pro softwarová omezení můžete aplikovat na všechny druhy spustitelných souborů kromě knihoven DLL nebo na veškerý software (viz obrázek 9.14). Výchozí možností je vynechat knihovny DLL, což většinou pro začátek postačí.



OBRAZEK 9.14: Práce s možnostmi vynucování v zásadách Software Restriction Policy

5. Máte možnost určovat, kdo bude zpracovávat zásady softwarových omezení. Implicitně jsou zásadami ovlivněni všichni uživatelé, ale pro jistotu můžete vymout členy skupiny Administrators místního počítače. Tak dosáhnete toho, že správci budou moci případně vrátit příliš restriktivní zásady.
6. Klepněte na tlačítko OK.

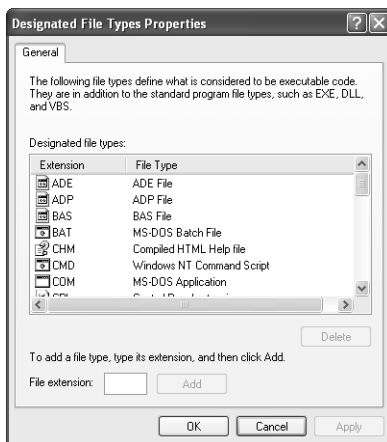


Upozornění Vzhledem k tomu, že zásady Software Restriction Policies dokáží zabránit spuštění souborů, měli byste jejich použití pečlivě naplánovat. Snadno se totiž můžete dostat do problémů v případě, že to s omezováním přeženete.

Prohlížení a konfigurování zásad Designated File Types

Zásady Designated File Types určují, které typy souborů a přípony jsou považovány za spustitelné soubory. Chcete-li prohlížet nebo nastavovat typy souborů, postupujte takto:

1. Podle potřeby nalistujte složku Computer Configuration\Windows Settings\Security Settings\Software Restrictions Policies nebo User Configuration\Windows Settings\Security Settings\Software Restrictions Policies a otevřete položku Software Restriction Policies.
2. Jestliže nejsou softwarová omezení zatím nastavena, klepněte pravým tlačítkem na uzel Software Restriction Policies a zvolte příkaz Create New Policies.
3. V pravém podokně klepněte pravým tlačítkem na položku Designated File Types a zvolte Properties.
4. V dialogu Designated File Types Properties (viz obrázek 9.15) se implicitně nachází seznam obvyklých přípon (např. .exe, .bat a .vbs).
5. Jestliže chcete do seznamu přidat nějaké přípony, můžete to udělat. Do pole File Extension zadejte novou příponu souboru, který je již v systému zaregistrován, a poté klepněte na tlačítko Add.
6. Spustitelné soubory můžete ze seznamu také odstraňovat. Vyberte typ souboru, který chcete odstranit, a poté klepněte na tlačítko Delete.
7. Klepněte na tlačítko OK.



OBRAZEK 9.15: Práce s typy souborů v zásadách Software Restriction Policy

Konfigurování zásad Trust Publisher

Pomocí zásad Trusted Publisher můžete spouštění softwaru povolit na základě podepsání spustitelného souboru veřejným klíčem. Můžete určit, zda běžní uživatelé mohou do seznamu důvěryhodných vydavatelů na jejich počítači přidávat nové položky, nebo zda bude tato akce povolena pouze správcům. Když například stáhnete soubor ze stránek firmy Microsoft, dostanete během stahování možnost přidat Microsoft do seznamu vydavatelů, které považujete za důvěryhodné.

Pomocí zásad Trusted Publisher můžete uživatelům zcela zabránit v přidávání důvěryhodných vydavatelů na jejich počítače. Tato možnost se vám může hodit, obzvláště když uživatele podezříváte z toho, že stahují software, který (i přesto, že je podepsaný) není vhodný pro použití na vašich počítačích. Tyto zásady můžete použít také k ověření toho, zda jsou certifikáty, které vydavatel použil k podepsání svého softwaru, stále platné. To se provádí kontrolou jejich certifikační autority a následným ověřením, zda nebyl certifikát zrušen – ať už kvůli vydavateli, nebo vypršení platnosti. Jedná se o dobrý přístup, ale může způsobit zhoršení odezvy, neboť systém Windows musí při každém použití certifikátu kontaktovat podpisovou autoritu, aby se ujistil, že certifikát je stále platný.

Chcete-li konfigurovat nebo prohlížet možnosti důvěryhodných vydavatelů, postupujte následovně:

1. Podle potřeby nalistujte složku Computer Configuration\Windows Settings\Security Settings\Software Restrictions Policies nebo User Configuration\Windows Settings\Security Settings\Software Restrictions Policies a otevřete složku Software Restriction Policies.
2. Jestliže nejsou softwarová omezení zatím nastavena, klepněte pravým tlačítkem na uzel Software Restriction Policies a zvolte příkaz Create New Policies.
3. V pravém podokně klepněte pravým tlačítkem na položku Trusted Publishers a zvolte Properties. Otevře se dialog Trusted Publishers.
4. Nastavte, kdo bude moci vybírat důvěryhodné vydavatele. Možnosti jsou následující:
 - **End Users** Důvěryhodné vydavatele mohou vybírat všichni uživatelé.
 - **Local Computer Administrator** Důvěryhodné vydavatele mohou vybírat pouze správci místního počítače (a doménoví nebo podnikoví správci).
 - **Enterprise Administrators** Důvěryhodné vydavatele mohou vybírat pouze členové skupin Domain Admins a Enterprise Admins.
5. Určete, zda se má kontrolovat případné zrušení certifikátu – z důvodu zrušení certifikátu vydavatelem, vypršení platnosti nebo z obou důvodů.
6. Klepněte na tlačítko OK.

Konfigurování nepovolených a neomezených aplikací

Prostřednictvím zásad Disallowed and Unrestricted Applications Security Levels můžete určovat, zda má být omezený software považován za nepovolený, nebo neomezený. Režimy se nazývají Disallowed (nepovoleno) a Unrestricted (neomezeno) a jsou jednoznačné. Implicitně je aktivní režim Unrestricted. To znamená, že všechny počítače a uživatelé podléhající těmto zásadám Software Restriction Policies mohou spouštět libovolné soubory kromě těch, které jsou explicitně blokovány vámi definovanými dodatečnými pravidly. Když je aktivní režim Disallowed, pak žádné počítače a žádní uživatelé podléhající těmto zásadám Software Restriction Policies nesmí spouštět žádné soubory kromě těch, které jsou explicitně povoleny prostřednictvím dodatečných pravidel.

Z toho vyplývá, že v rámci zásad Security Levels máte na výběr buď blokovat vše a povolit jen známé výjimky, nebo povolit vše a blokovat jen soubory, o kterých ví-

te, že nejsou bezpečné. Ideální volba se odvíjí od vašich nároků na zabezpečení, ale v případě, že jako výchozí režim použijete volbu Disallowed, budou mít vaši správci mnohem více práce, aby vyhověli potřebám uživatelů s požadavky na použití dodatečných aplikací. Jestliže máte ale pečlivě řízené a statické prostředí, bude to výborná volba, která zabrání uživatelům ve spouštění neznámých, potenciálně škodlivých souborů.

Chcete-li nastavit úroveň zabezpečení, postupujte takto:

1. Podle potřeby nalistujte složku Computer Configuration\Windows Settings\Security Settings\Software Restrictions Policies nebo User Configuration\Windows Settings\Security Settings\Software Restrictions Policies a otevřete položku Software Restriction Policies.
2. Jestliže nejsou softwarová omezení zatím nastavena, klepněte pravým tlačítkem na uzel Software Restriction Policies a zvolte příkaz Create New Policies.
3. Označte uzel Security Levels. Ikona aktuálně zvolené výchozí možnosti je zobrazena se zeleným kroužkem a „fajfkou“.
 - Chcete-li, aby výchozí úroveň zabezpečení byl režim Disallowed (Nepovoleno), klepněte pravým tlačítkem na položku Disallowed a zvolte Set As Default.
 - Chcete-li, aby výchozí úroveň zabezpečení byl režim Unrestricted (Bez omezení), klepněte pravým tlačítkem na položku Unrestricted a zvolte Set As Default (Nastavit jako výchozí).

Konfigurování pravidel zabezpečení

Pomocí zásad Additional Rules můžete nakonfigurovat pravidla určující, který software bude blokován a který bude možné spouštět. Když klepnete pravým tlačítkem na uzel Additional Rules, máte na výběr ze čtyř druhů pravidel:

- Certificate Rules (Pravidla certifikátu)
- Hash Rules (Pravidla algoritmu hash)
- Internet Zone Rules (Pravidla zóny Internetu)
- Path Rules (Pravidla cesty)

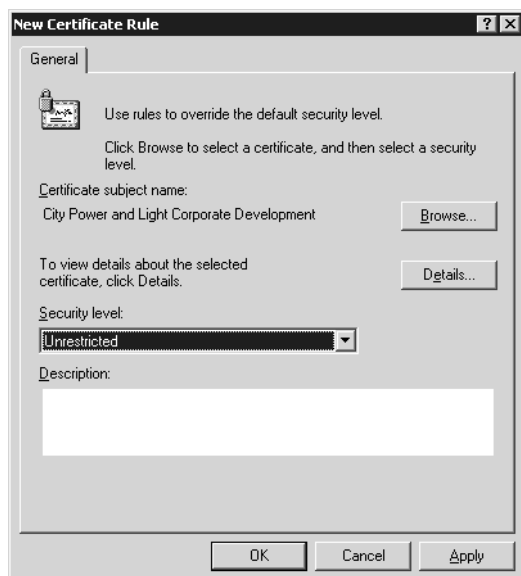
Následující oddíly se zabývají tím, jak jednotlivá pravidla použít v zásadách Software Restriction Policies.

Certificate Rules Tato pravidla vám umožňují povolit či zakázat spouštění souborů na základě digitálních podpisů. Jestliže například váš interní vývojářský tým podepisuje všechny vytvořené aplikace, můžete vytvořit certifikační pravidlo, které povolí běh všech takto podepsaných aplikací (viz obrázek 9.16).

Chcete-li vytvořit certifikační pravidlo, postupujte následovně:

1. Podle potřeby nalistujte složku Computer Configuration\Windows Settings\Security Settings\Software Restrictions Policies nebo User Configuration\Windows Settings\Security Settings\Software Restrictions Policies a otevřete položku Software Restriction Policies.
2. Klepněte pravým tlačítkem na položku Additional Rules a zvolte příkaz New Certificate Rule.

3. V dialogu New Certificate Rule klepněte na tlačítko Browse a nalistujte certificační soubor.
4. Prostřednictvím seznamu Security Level určete, zda aplikace podepsané tímto certifikátem budou nepovolené, nebo neomezené.
5. Klepněte na tlačítko OK.



OBŘÁZEK 9.16: Tvorba certificačního pravidla v zásadách Software Restriction Policy

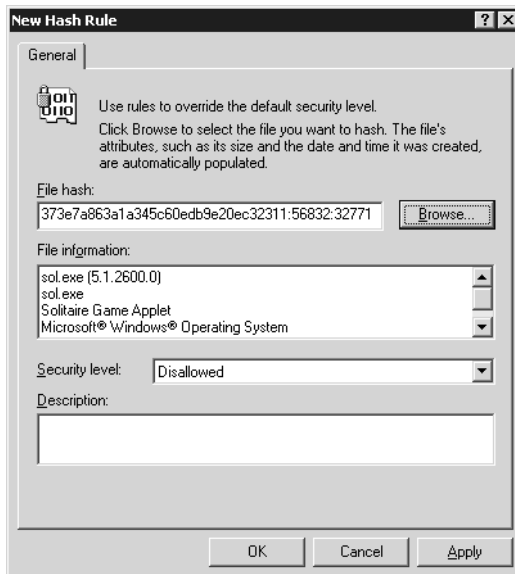
Hash Rules Hodnoty hash souborů jsou jednoznačné, neopakovatelné hodnoty, které se vypočítávají na základě obsahu souboru. Vytvořením pravidla hash můžete omezit nebo povolit spouštění jednotlivých verzí souborů.

Chcete-li vytvořit pravidlo hash, postupujte následovně:

1. Podle potřeby nalistujte složku Computer Configuration\Windows Settings\Security Settings\Software Restrictions Policies nebo User Configuration\Windows Settings\Security Settings\Software Restrictions Policies a otevřete položku Software Restriction Policies.
2. Klepněte pravým tlačítkem na položku Additional Rules a zvolte příkaz New Hash Rule.
3. V dialogu New Hash Rule klepněte na tlačítko Browse a nalistujte spustitelný soubor, který chcete řídit, a vyberte jej. Jak vidíte na obrázku 9.17, hash souboru se automaticky vypočte.
4. Pomocí seznamu Security Level určete, zda aplikace podepsané tímto certifikátem budou nepovolené, nebo neomezené.
5. Klepněte na tlačítko OK.



Poznámka Na obrázku 9.17 jsme vytvořili pravidlo hash, které zabrání ve spuštění programu Solitaire. Protože je pravidlo založeno na hodnotě hash souboru, může uživatel soubor Sol.exe přejmenovat na cokoliv jiného a ten zůstane i nadále blokován.



OBRAZEK 9.17: Vytvoření pravidla hash v zásadách Software Restriction Policy

Internet Zone Rules Pravidlo zóny Internet vám umožňuje řídit spuštění souborů na základě toho, odkud jsou spouštěny. Toto pravidlo podporuje kontrolu poskytovanou aplikací Microsoft Internet Explorer tím, že vám umožňuje řídit soubory nainstalované prostřednictvím Instalační služby systému Windows. To znamená, že toto pravidlo platí pouze pro aplikace, které byly nainstalovány prostřednictvím balíčku Instalační služby systému Windows z určitého síťového umístění. Jestliže se uživatel například pokusí spustit instalaci aplikace pomocí balíčku Instalační služby systému Windows staženého z Internetu, může toto pravidlo takové instalaci zabránit.

Pravidla Internet Zone Rules můžete v podstatě použít k řízení toho, jaký software a odkud může uživatel instalovat. Tato pravidla ale bohužel nemají vliv na software, který je v jiném formátu než v balíčku Instalační služby systému Windows.

Chcete-li vytvořit pravidlo zóny Internet, postupujte následovně:

1. Podle potřeby nalistujte složku Computer Configuration\Windows Settings\Security Settings\Software Restrictions Policies nebo User Configuration\Windows Settings\Security Settings\Software Restrictions Policies a otevřete položku Software Restriction Policies.
2. Klepněte pravým tlačítkem na položku Additional Rules a zvolte příkaz New Internet Zone Rule.
3. Pomocí seznamu Internet Zone určete zónu, kterou chcete konfigurovat. Zóny jsou:
 - Local Computer

- Local Intranet
 - Restricted Sites
 - Trusted Sites
 - Internet
4. Pomocí seznamu Security Level určete, zda aplikace z této zóny budou nepovolené, nebo neomezené.
 5. Klepněte na tlačítko OK.

Path Rules Tato pravidla jsou z pohledu povolování a zakazování spouštění souborů pravděpodobně neflexibilnější. Stačí zadat cestu souborového systému k souboru či složce a veškeré soubory spadající pod nastavení Designated File Types budou tímto pravidlem řízeny. Počítejte s tím, že vámi zadaná cesta je rekurzivní. To znamená, že jestliže zadáte například `c:\program files`, budou řízeny všechny soubory a složky nacházející se v tomto rodičovském adresáři. Proto si dávejte pozor, až budete aplikovat zákaz pro větší hierarchii složek.

Pravidla Path Rules můžete vytvářet i pro klíče registru. To se může hodit v případě, že chcete kontrolovat, co bude možné spouštět z různých míst registru pro automatické spouštění (příkladem může být klíč RunOnce). Nejzrádnější částí konfigurace cesty registru je to, že cesty registru nemůžete v dialogu Path Rule procházet. Namísto toho musíte cestu ke klíči registru psát do pole Path ručně nebo ji pomocí funkce kopírovat/vložit zkopírovat z programu Editor registru. Cestu registru musíte navíc uzavřít mezi znaky %, viz níže:

```
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce%
```

Tím, že omezíte obvyklé cesty registru provádějící úlohy automatického spouštění, můžete řídit nebezpečné soubory, které by se mohly na pracovní stanici uživatele pokusit o instalaci sebe sama.

Chcete-li vytvořit pravidlo cesty, postupujte následovně:

1. Podle potřeby nalistujte složku Computer Configuration\Windows Settings\Security Settings\Software Restrictions Policies nebo User Configuration\Windows Settings\Security Settings\Software Restrictions Policies a otevřete položku Software Restriction Policies.
2. Klepněte pravým tlačítkem na položku Additional Rules a zvolte příkaz New Path Rule.
3. Napište cestu, kterou chcete použít. Také můžete klepnout na tlačítko Browse a nalistovat soubor či složku, kterou chcete řídit, a vybrat ji. U cest registru musíte zadat cestu do pole Path ručně nebo ji zkopírovat z nástroje Editor registru.



Poznámka Nezapomeňte na to, že cestu registru je potřeba uzavřít mezi symboly % (jak bylo uvedeno výše).

4. Pomocí seznamu Security Level určete, zda aplikace z tohoto umístění budou nepovolené, nebo neomezené.
5. Klepněte na tlačítko OK.

Řešení problémů se zásadami Software Installation Policy

Pro zajištění správného fungování zásad Software Installation (Instalace softwaru) je k dispozici mnoho nástrojů a technik. Hlavními nástroji jsou různé protokolovací soubory, které můžete zapnout, abyste získali informace o tom, co se děje během zpracování zásad Software Installation. Mezi hlavní protokolovací soubory patří:

- **Protokol událostí aplikace** Tento protokol zaznamenává na cílovém počítači zprávy související s obecným zpracováním zásad skupiny a také zprávy související s instalací softwaru. Zdrojem zpráv souvisejících se zásadami Software Installation jsou zásady Application Management nebo služba AppMgmt. Zdrojem zpráv spojených s Instalační službou systému Windows je proces MsiInstaller. Tyto zprávy vám říkají, zda byla instalace aplikace úspěšná, a v případě, že nebyla, poskytnou vám protokol obvykle nějaké základní vysvětlení.
- **%windir%\debug\usermode\userenv.log** Poskytuje informace o problémech se zpracováním zásad skupiny a o chybových kódech vyšší úrovně souvisejících se zpracováním zásad Software Installation. Může vám také pomoci zjistit, proč nedošlo během určitého procesního cyklu ke zpracování určitého objektu GPO.
- **%windir%\Debug\UserMode\apppgmt.log** Podrobně zaznamenává kroky zpracování zásad Software Installation, včetně toho, které objekty GPO jsou zpracovávány a které aplikace se instalují.
- **%temp%\msi*.log** Jádro Instalační služby systému Windows dokáže vytvářet podrobné protokoly, které obsahují všechny kroky provedené během instalace balíčku. Tento protokol je užitečný při řešení problémů souvisejících s balíčkem, když jste si jisti, že zpracování zásad Software Installation probíhá správně, ale aplikaci se nedaří nainstalovat. U zavádění pro jednotlivé počítače se tyto protokoly vytvářejí s jednoznačným názvem souboru ve formátu `msi*.log` a nacházejí se ve složce `%windir%\temp`. U instalací pro jednotlivé uživatele se protokoly vytvářejí v uživatelské složce `%temp%`.

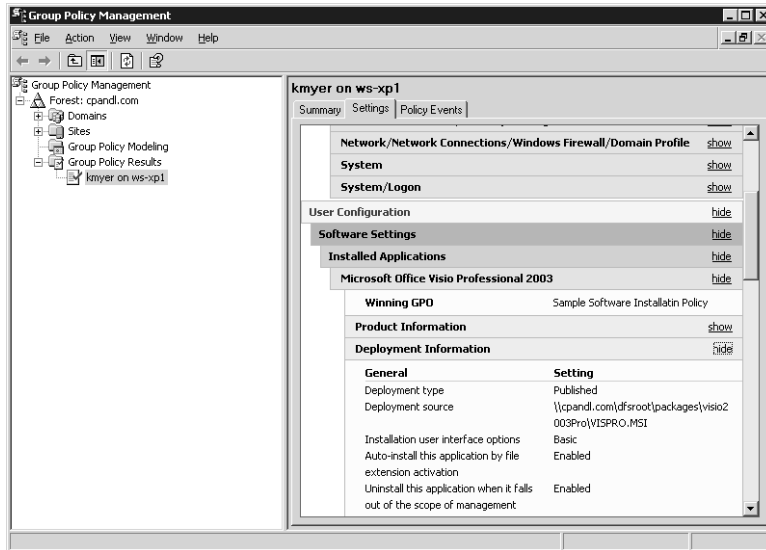
Tyto protokoly jsou uloženy na klientských počítačích, které zpracovávají zásady Software Installation, nikoliv na doménovém řadiči. Chcete-li se dozvědět více o tom, jak tyto protokoly využívat, přečtěte si 16. kapitolu.

Kromě protokolů můžete při hledání informací využít i průvodce Group Policy Results Wizard, nacházejícího se v konzole Group Policy Management Console, který dokáže informace o zpracování zásad Software Installation sbírat ze vzdálených počítačů a ověřovat, zda byla aplikace nainstalována podle očekávání. Obrázek 9.18 ukazuje příklad zprávy o nastaveních vygenerované tímto průvodcem. Průvodce také obsahuje filtrovaný náhled na protokol událostí aplikací klientského počítače, který z karty Policy Events ukazuje pouze události související se zásadami skupiny.

Řešení problémů

První věcí, kterou můžete udělat v zájmu toho, abyste pochopili, co se děje během zpracování zásad Software Installation (Instalace softwaru), je zapnout podrobné evidování zpráv o stavu zásad skupiny. Docílíte toho tak, že ve složce `Computer Configuration\Administrative Templates\System` zapnete nastavení `Verbose Vs`.

Normal Status Messages (Konfigurace počítače\Šablony pro správu\System – Podrobné nebo normální zprávy o stavu).



OBRÁZEK 9.18: Prohlížení informací o zásadách Software Installation prostřednictvím zprávy průvodce Group Policy Results

Zapnutím těchto zásad získáte přehled o tom, co se děje během zpracování zásad skupiny na popředí včetně toho, kdy se spravované aplikace instalují a která instalace právě probíhá.

Pomocí výše uvedených nástrojů a protokolů se dá dobře aplikovat následující přístup k řešení problémů souvisejících se zpracováním zásad Software Installation:

1. Jestliže se aplikaci nepodaří pro cílového uživatele či počítač správně nainstalovat, použijte průvodce Group Policy Results Wizard konzoly GPMC a ujistěte se, že uživatel či počítač opravdu zpracovává objekt GPO, který obsahuje aplikační balíček. Jestliže zjistíte, že ne, pak se obraťte na 17. kapitolu, kde najdete možná řešení.
2. Jestliže jste si ověřili, že objekt GPO se zpracovává, ale aplikaci se přesto nedaří nainstalovat, je potřeba zapnout protokolování, abyste mohli určit, kde dochází k chybě. Nejprve zapněte protokol `Appmgmt.log`, který vám pomůže zjistit, zda k pokusu o instalaci vůbec dochází a zda nastaly nějaké chyby. Tento soubor obvykle obsahuje chybové kódy související s instalací nebo poskytuje informace o příčině selhání instalace.
3. Jestliže protokol `Appmgmt.log` obsahuje informace o tom, že instalace byla zahájena, ale selhala, je dalším krokem zapnutí podrobného protokolování Instalační služby systému Windows. Soubor protokolu vygenerovaný během instalace obsahuje všechny akce provedené balíčkem a může vám poskytnout velice cenné informace o tom, kde a proč k selhání dochází.

Obvyklé problémy se zásadami Software Installation

Hoďně komplikací, ke kterým dochází při zpracování zásad Software Installation (Instalace softwaru), lze vyřešit relativně snadno. Nejčastější z nich jsou popsány níže:

- **Pro spuštění instalace pomocí zásad je potřeba dvou až tří restartů počítače resp. přihlášení uživatele.** Jestliže máte na svých klientských počítačích operační systém Windows XP, pak mají pravděpodobně zapnutou funkci Fast Logon Optimization. Ta může způsobit, že ke zpracování některých zásad skupiny (např. právě zásad Software Installation) je potřeba několika restartů či přihlášení. Tuto funkci můžete vypnout tak, že ve složce Computer Configuration\Administrative Templates\System\Logon zapnete nastavení Always Wait For The Network At Computer Startup And Logon (Při spouštění a přihlašování počítače vždy počkat na síť).
- **Zásady Software Installation nejsou zpracovány, ačkoliv ostatní zásady jsou zpracovány bez problémů.** Jak již bylo řečeno dříve, zásady Software Installation se implicitně nezpracovávají v případě, že bylo detekováno pomalé připojení mezi počítačem a doménovým řadičem. Chcete-li ověřit, zda nebylo zjištěno pomalé připojení, spusťte pro daného klienta průvodce Group Policy Results Wizard konzoly GPMC. Ten vám řekne, zda během posledního cyklu zpracování zásad na popředí došlo k detekování pomalého připojení.
- **Uživatelé či počítače nemohou spustit instalační program aplikace a zobrazuje se jim chyba „Access Denied“** Aby bylo možné spustit instalační program, musí mít počítač či uživatel oprávnění pro čtení souborů a sdílené složky, v níž se nachází balíček Instalační služby systému Windows. Zajistěte, aby uživatelé a počítače, kteří zásady zpracovávají, měli dostatečná oprávnění pro přístup k instalačním balíčkům.
- **Zásady Software Installation před nainstalováním nové kopie aplikace z počítačů odinstalují existující verzi softwaru.** K tomu může vzhledem k principu fungování celého procesu opravdu dojít. Jestliže zásady Software Installation najdou na počítači aplikaci, která byla nainstalována ručně mimo zásady Software Installation, a tato aplikace má stejný produktový kód Instalační služby systému Windows jako spravovaná aplikace, která se má instalovat, pak se ručně nainstalovaná aplikace automaticky odinstaluje. Tím je zajištěno, že na vašich systémech jsou nainstalovány pouze spravované aplikace.
- **Jeden ze správců ručně odinstaloval aplikaci, která byla předtím zavedena prostřednictvím zásad Software Installation. Když počítač znovu zpracuje tyto zásady, aplikace se již znovu nenainstaluje.** Spravované aplikace zavedené pomocí zásad Software Installation by se nikdy neměly odstraňovat ručně. Přestože je samotná aplikace odstraněna, v registrech zůstanou informace, které způsobí, že zásady Software Installation jsou i nadále přesvědčené o tom, že aplikace je stále nainstalovaná. V případě nutnosti můžete tyto informace ručně smazat a vynutit tak reinstalaci. V nástroji Editor registru otevřete HKEY_CURRENT_USER\Software\Microsoft\Windows\Current-Version\Group Policy\AppMgmt (nebo použijte větev HKEY_LOCAL_MACHINE v případě, že aplikace byla zaváděna pro jednotlivé počítače). V této větvi má každá spravovaná aplikace svůj klíč,

který obsahuje zaváděcí informace. Najděte odpovídající klíč, který obsahuje odinstalovanou aplikaci, a smažte jej.

9.7 Shrnutí

Zásady Software Installation vám v rámci oddělení umožňují pro uživatele a počítače snadno zavádět software. Aplikace můžete publikovat nebo přiřazovat uživatelům a počítačům. Když zásady Software Installation použijete spolu s Instalační službou systému Windows, můžete ve svém prostředí spravovat celý životní cyklus aplikací – instalaci, opravy, aktualizace, záplatování a odstraňování. S pomocí zásad Software Restriction můžete spravovat nejenom software nainstalovaný na uživatelských stanicích, ale můžete také zajistit, že se ve vašem prostředí bude spouštět pouze autorizovaný software. Tyto zásady dohromady poskytují velmi silný nástroj pro zajišťování bezpečného a řízeného prostředí, v němž mohou být vaši uživatelé maximálně produktivní.