KAPITOLA 4

Sestavování a správa webových aplikací

V této kapitole:

Architektura webové aplikace....134
Vytváření a rozšiřování webových aplikací....139
Správa webových aplikací....152
Mapování alternativních adres URL....162

Webové aplikace tvoří vrchol hierarchie na úrovni farmy a jsou základem pro jakoukoli implementaci systému Microsoft SharePoint Server 2010. Webové aplikace systému SharePoint Server 2010 se od většiny webů liší tím, že obsah se nachází v databázi, a ne v souborovém systému webového serveru. Na serveru SharePoint existuje jen minimální obsah nezbytný pro připojení serveru služby IIS (Internet Information Services) k databázím. Logická struktura webové aplikace se tak celá nachází v databázích Microsoft SQL Server. Konfigurace webové aplikace je uložená v konfigurační databázi. Uživatelský obsah webové aplikace je uložen v jedné či více obsahových databázích.

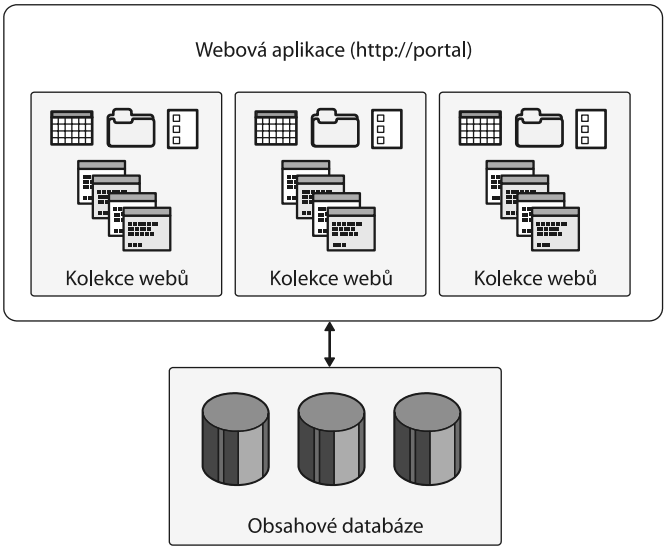
Z hlediska fyzické architektury představují webové aplikace specifický webový a aplikační obor služby IIS poskytující koncovým uživatelům možnost interakce s obsahem přes adresy URL (Uniform Resource Locator). Koncový uživatel nemá vizuální reprezentaci webové aplikace. Ta je zcela spravována na úrovni farmy Centrální správou nebo pomocí prostředí Microsoft Windows PowerShell. Pro základní administrativní činnosti farmy lze i tak použít nástroj pro správu `stsadm.exe`, který je však v následující verzi systému SharePoint navržený pro odstranění. Proto by bylo rozumné zahájit přechod na prostředí Windows PowerShell.

Architektura webové aplikace

Webovou aplikaci lze vytvořit z Centrální správy, přičemž dojde ke spojení webu služby IIS s alespoň jednou obsahovou databází vytvořenou ve vaší implementaci SQL Serveru. Pamatujte si, že nová webová aplikace je prázdná skořápka, která ve výchozím stavu neobsahuje žádné kolekce webů. Při pokusu o otevření webové aplikace před vytvořením kolekce webů uvidíte stránku s chybou 404 (Page Not Found).

Poznámka: Služba IIS vytváří web pro každou webovou aplikaci vytvořenou v systému SharePoint. Systém SharePoint pak vytváří v rámci webových aplikací kolekce webů.

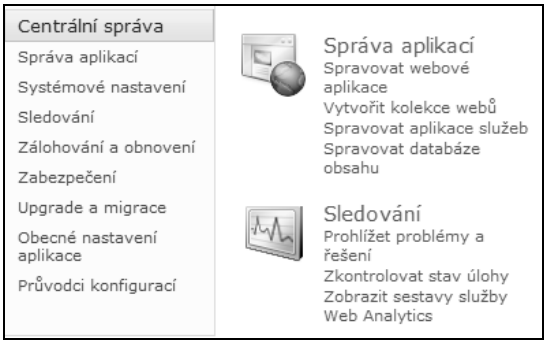
Pokud použijete Průvodce konfigurací farmy, provede vás tento průvodce přes kroky pro vytvoření první webové aplikace a také první kolekce webů. Obrázek 4.1 znázorňuje vztah mezi kolekcemi webů, webovými aplikacemi a obsahovými databázemi.



Obrázek 4.1: Vztah mezi webovými aplikacemi, kolekcemi webů a obsahovými databázemi

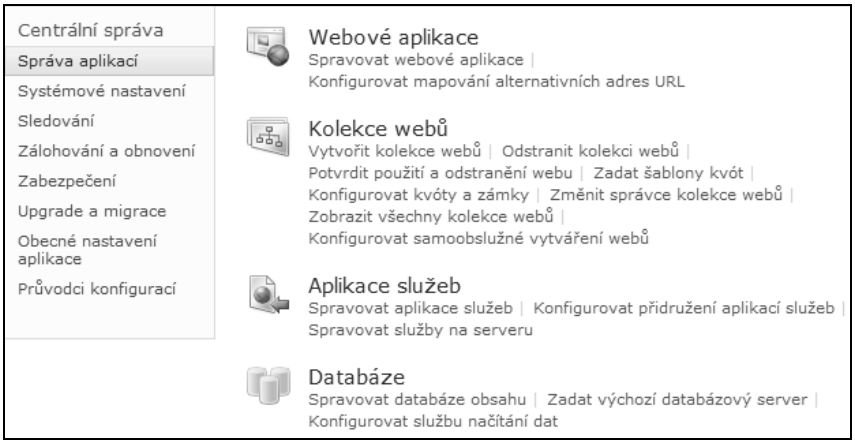
Správa webové aplikace

Webové aplikace lze spravovat pomocí Centrální správy. K tomuto účelu slouží dva odkazy. První je umístěný na úvodní stránce Centrální správy v části **Správa aplikací** (viz obrázek 4.2).



Obrázek 4.2: Odkaz Spravovat webové aplikace je umístěn na úvodní stránce Centrální správy

Odkaz **Spravovat webové aplikace** můžete najít v Centrální správě také na stránce části **Správa aplikací**, kde se nachází seskupení **Webové aplikace** (viz obrázek 4.3).

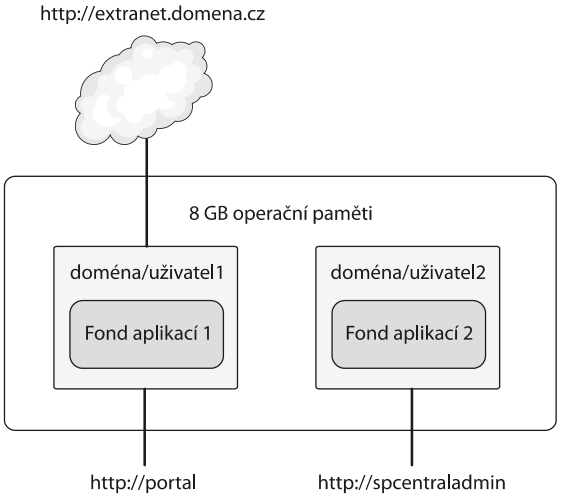


Obrázek 4.3: Odkaz Spravovat webové aplikace se nachází též na stránce Správa aplikací

Fondy aplikací

Fond aplikací služby ISS je izolovaný paměťový prostor, který je směrován do jednoho či více pracovních procesů uvnitř kontextu zabezpečení daného uživatele. Pracovní proces (`w3wp.exe`) spouští webové aplikace a obsluhuje požadavky zaslané serveru pro určitý fond aplikací. Webová aplikace s vlastním fondem aplikací nebude ovlivněna problémy s jinými aplikacemi v odděleném fondu aplikací. Na obrázku 4.4 používají dvě webové aplikace (*https://portal.domena.cz* a *http://portal*) tentýž fond aplikací. Takové sdílení fondu aplikací na jednu stranu snižuje nároky na paměť, ale na druhou stranu přináší riziko havárie obou webových aplikací v případě,

kdy jedna z nich kvůli špatně napsanému kódu nebo kompromitovanému serveru havaruje.



Obrázek 4.4: Fondy aplikací hostující webové aplikace v paměti

Implementování různých fondů aplikací a uživatelským jmen (identit) pro každou webovou aplikaci vaši celkovou bezpečnostní pozici sice posílí, avšak každý další fond aplikací vyžaduje více paměti. Je-li to možné, měli byste pro izolaci použít samostatný fond webových aplikací, a to i tehdy, budou-li oba fondy používat tutéž identitu.

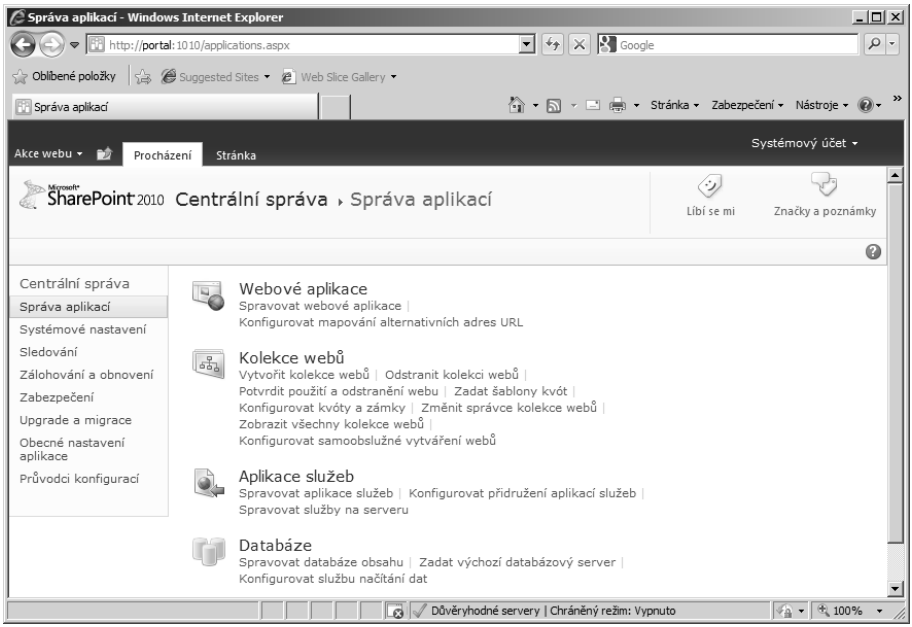
Rozhodnutí, zda použít, či nepoužít více identit fondu aplikací, závisí na úrovni zabezpečení, kterou požaduje vaše organizace. Obecně lze říci, že webové aplikace se stejnou úrovní zabezpečení sdílejí jednu identitu fondu aplikací. V opačném případě se můžete rozhodnout provést instalaci s jedním či několika účty pro fondy aplikací služby IIS a databázový přístup. Je totiž mnohem snazší provést na začátku instalaci se samostatnými účty než později měnit a izolovat fondy aplikací.

Obsahové databáze

Obsahové databáze zahrnují obsah všech kolekcí webů, včetně většiny přizpůsobení provedených v prohlížeči nebo v nástroji SharePoint Designer. Ve výchozím stavu se pro jednu webovou aplikaci vytvoří jedna obsahová databáze. Další obsahové databáze byste měli vytvořit pro omezení velikosti současných obsahových databází nebo pro izolování na fyzickém disku SQL Serveru. Je-li například kvóta vaší webové kolekce 10 GB a přitom chcete omezit velikost vaší obsahové databáze na 100 GB, musíte vytvořit obsahovou databázi pro každých 10 kolekcí webů v přidružené webové aplikaci.

Tip: Obsahová databáze obsahuje kolekci webů. Obsahovou databázi spojenou s webovou aplikací 1 lze odebrat a spojit s webovou aplikací 2. Veškeré kolekce webů v datové sadě tohoto obsahu pak budou k dispozici pro webovou aplikaci 2 pod její původní spravovanou cestou. Výjimka nastává ve chvíli, kdy se daná adresa URL již používá, což se děje třeba v případě spravované kořenové cesty.

Pro správu obsahových databází otevřete jako na obrázku 4.5 v Centrální správě část **Správa aplikací**, **Databáze**, **Spravovat databáze obsahu**.



Obrázek 4.5: Umístění odkazu Spravovat databáze obsahu v Centrální správě

Přes rozhraní **Spravovat databáze obsahu** můžete přidávat další databáze. Zde můžete přidat či spravovat obsahové databáze a dále jako na obrázku 4.6 prohlížet informace o obsahové databázi.

Obrázek 4.6: Rozhraní Manage Content Databases

Pro každou obsahovou databázi je k dispozici sedm hlavních vlastností:

- **Informace o databázi** – část s informacemi o databázi zobrazuje název databázového serveru, název databáze a stav. Změna stavu na hodnotu **Režim offline** zamezí vytváření nových kolekcí webů v této obsahové databázi. Dále se zde zob-

razuje typ autentizace, který byl definován při vytváření přidružené webové aplikace, jedná-li se o první obsahovou databázi, nebo během tvorby obsahové databáze pro následné databáze.

Důležité: Pro zamezení vytváření kolekcí webů v dané databázi nastavte maximální počet webů na aktuální počet uložený v databázi. Důvodem je to, že databáze v režimu offline měly v předchozí verzi systému SharePoint Server určité problémy, které se mohou opakovat i ve verzi 2010. Je třeba poznamenat, že toto rozhraní se neodkazuje na podřízené weby, ale na kolekce webů.

- **Správa verzí a upgrade databází** – tato vlastnost je v systému SharePoint Server 2010 nová. Je užitečná při upgradu databází na novou verzi systému SharePoint. Zobrazí aktuální verzi opravy a také verzi systému SharePoint Server. Ať už jste provedli upgrade ze systému SharePoint Server 2007, nebo ne, tato stránka zobrazí databáze a informace související s aktualizacemi.
- **Server s podporou převzetí služeb při selhání** – jedná se o novou funkci systému SharePoint Server 2010 pro podporu zrcadlení databáze SQL. Konfigurace tohoto nastavení nezpůsobí konfiguraci zrcadlení databáze, ale jen připraví systém SharePoint Server 2010 na to, aby si byl zrcadlení vědom. Pro úspěšné dokončení konfigurace musíte nakonfigurovat zrcadlení databáze v aplikaci SQL Server Management Studio.
- **Nastavení kapacity databáze** – měli byste provést odborné rozhodnutí ohledně toho, jaké hodnoty použít pro nastavení Počtu webů před vytvořením upozorňovací události a Maximálního počtu webů, které lze vytvořit v této databázi. Pokud například nechcete, aby vaše obsahové databáze byly větší než 100 GB, a kvóty pro vaše weby jsou nastaveny na 1 GB, pak musíte změnit maximální počet webů na 100. Výchozí nastavení jsou téměř vždy příliš vysoká, a měli byste je tedy změnit. Je třeba poznamenat, že tato obrazovka se neodkazuje na podřízené weby, ale na kolekce webů.
- **Search Server** – používáte-li systém SharePoint Server 2010, pak můžete nastavení pro vyhledávací server bezpečně ignorovat. Používá se totiž pouze v instalaci systému SharePoint Foundation 2010, kde není vyhledávací služba dostupná.
- **Odebrat databázi obsahu** – odebrání obsahové databáze způsobí zrušení spojení databáze s webovou aplikací, ale nezpůsobí její vymazání z SQL Serveru. Téměř nikdy není důvod pro odebrání obsahové databáze bez odebrání celé webové aplikace. Můžete tak ovšem učinit v případě nutnosti okamžitého odpojení citlivých dat bez jejich ztráty nebo při opětovném spojení obsahové databáze s novou webovou aplikací. Při odebírání obsahové databáze zůstanou všechna data v databázi a lze je tak připojit k jiné webové aplikaci a skrze ni k nim přistupovat. Opětovné přidružování obsahových databází k jiné webové aplikaci byste měli provádět pouze po důkladném otestování v laboratoři.
- **Preferovaný server pro úlohy časovače** – nová možnost systému SharePoint Server 2010, která podporuje separaci služeb na různých serverech. Kupříkladu

Služba Timer systému SharePoint 2010 provádí kroky pracovního postupu při jejich pokračování ze zpožďovací vrstvy nebo z události přijaté na jiném místě.

Vytváření a rozšiřování webových aplikací

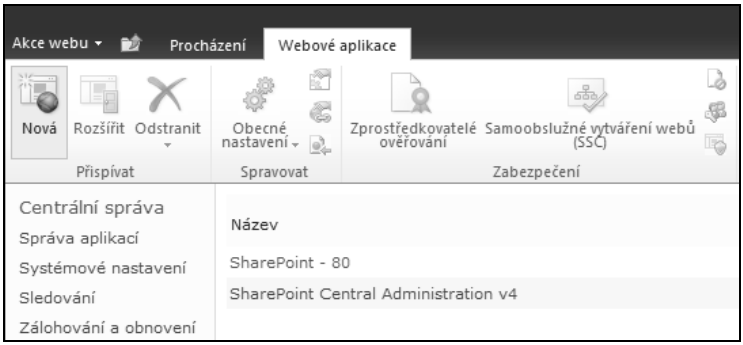
Tvorba webových aplikací je jedním z nejzákladnějších a nejpodstatnějších aspektů při správě produktů SharePoint. Webová aplikace poskytuje rozhraní pro interakci s uživateli skrze jejich prohlížeče. Webové aplikace jsou kombinací virtuálních serverů služby IIS, přidružených obsahových databází a záznamů pro tyto servery i databáze v konfigurační databázi.

Vytvoření webové aplikace

Před vytvořením webové aplikace zkontrolujte, že je počáteční konfigurace správná. Řada nastavení, jako jsou ta pro hlavičku hostitele, nelze po vytvoření webové aplikace změnit. Přestože nastavení můžete upravit ve službě IIS, v konfigurační databázi je změnit nelze. Veškerá nastavení zadaná v Centrální správě se zapisují do konfigurační databáze a použijí se při přidávání nových serverů do farmy. Je-li konfigurace nesprávná, musíte si pamatovat, že je nutné ručně aktualizovat každý nový server přidávaný do farmy a také stávající servery, pokud restartujete službu Microsoft SharePoint Foundation Web Application.

Pro vytvoření nové webové aplikace proveďte následující:

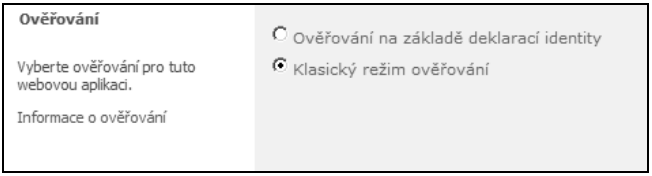
1. V Centrální správě otevřete **Správu aplikací**, **Webové aplikace**, **Spravovat webové aplikace** a poté na pásu karet klepněte na tlačítko **Nová** (viz obrázek 4.7).



Obrázek 4.7: Tlačítko Nová na pásu karet se používá k vytvoření nové webové aplikace

2. Dále vyberte typ ověřování pro tuto webovou aplikaci. Pokud vaše organizace nevyužívá možnost **Ověřování na základě deklarací identity**, vyberte jako na obrázku 4.8 možnost **Klasický režim ověřování**. Změna výběru typu autentizace způsobí obnovení dialogu a zobrazení různých možností v dialogovém okně **Vytvořit novou webovou aplikaci**.

- **Ověřování na základě deklarací identity** – jedná se o novou funkci systému SharePoint Server 2010, která je postavená na technologii WIF (Windows Identity Foundation). Používá identitu uživatele společně s dalšími podrobnostmi, které mohou pocházet z organizace uživatele, jiných organizací nebo z Internetu. Umožňuje autentizaci mezi systémy na bázi Windows a systémy, které nejsou založené na Windows. Ověřování na základě deklarací identity je flexibilní framework založený na standardních tokenech jazyka SAML (Security Assertion Markup Language), nejedná se však o skutečné prostředky autentizace.



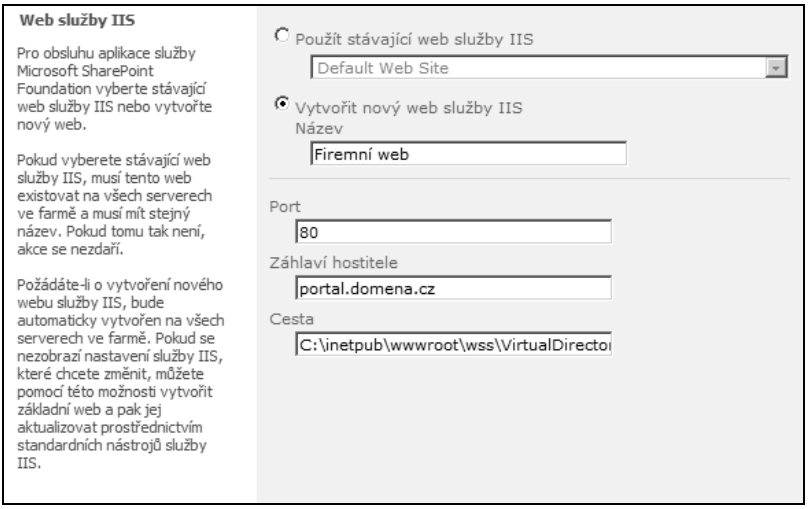
Obrázek 4.8: Možnosti ověření pro webovou aplikaci

Tip: Pokud provádíte upgrade ze systému SharePoint Server 2007 a používali jste autentizaci na bázi formulářů nebo webovou autentizaci typu SSO (Single Sign-On), pak musíte před použitím webových aplikací systému SharePoint Server 2010 přejít na deklarovanou autentizaci.

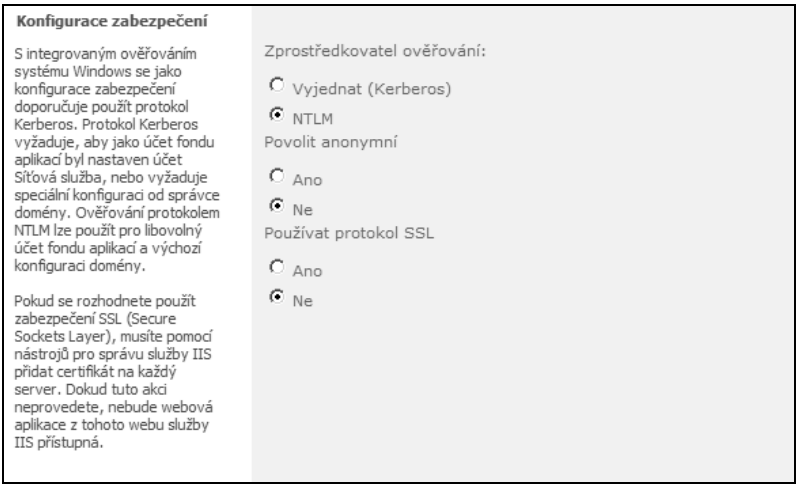
- **Klasický režim ověřování** – tento režim v podstatě používá pro webové aplikace systému SharePoint Server 2010 autentizaci služby IIS. Pokud chcete jednoduše použít Kerberos nebo NTLM, vyberte možnost **Klasický režim ověřování**. Je třeba poznamenat, že základní autentizaci lze nakonfigurovat po vytvoření webové aplikace, avšak ne během její tvorby. Při využívání základní autentizace používejte vždy protokol SSL (Secure Sockets Layer).

3. Dále je nutné vytvořit nový web služby IIS. Pokud vyberete možnost **Použít stávající web služby IIS**, načte webová aplikace konfiguraci služby IIS pro server provozující Centrální správu. Toto nastavení se požívá jen zřídkakdy a obvykle má za úkol opravit porušenou webovou aplikaci. Pro tento příklad vyberte možnost **Vytvořit nový web služby IIS**. Zvolte jméno, které bude možné ve Správci služby IIS snadno identifikovat. Možnosti **Web služby IIS**, **Port**, **Záhlaví hostitele** a **Cesta** jsou zachycené na obrázku 4.9.
4. Po definování názvu webu služby IIS musíte definovat číslo portu. Obvykle se jedná o port 80 pro protokol HTTP nebo 443 pro protokol HTTPS.
5. Dále definujte hlavičku hostitele pro webovou aplikaci. Obvykle by mělo jít o plně kvalifikovaný název domény pro webovou aplikaci. Tuto hodnotu je sice možné později změnit ve službě IIS na každém serveru farmy, v konfigurační databázi ji však změnit nelze. Musíte tedy správně nakonfigurovat hlavičku hostitele již při vytváření webové aplikace.

Důležité: Během tvorby webové aplikace lze definovat pouze jednu hlavičku hostitele. Pokud potřebujete více hlaviček hostitelů (např. *http://portal* a *http://portal*), pak musíte přidat další ve službě IIS na každém serveru farmy.



Obrázek 4.9: Výchozí nastavení konfigurace webu služby IIS



Obrázek 4.10: Výchozí nastavení konfigurace zabezpečení pro autentizaci v klasickém režimu

6. Definujte cestu pro web. Nemáte-li nařízeno používat jiná nastavení nežli výchozí, měla by výchozí nastavení fungovat správně. Pokud musíte změnit cestu, zkontrolujte, že písmeno disku existuje na každém webovém serveru farmy.

V opačném případě by vytvoření webové aplikace selhalo na serverech, které dané písmeno disku nemají.

7. V závislosti na zvoleném typu autentizace se pro konfiguraci zabezpečení zobrazí jedna z následujících možností:

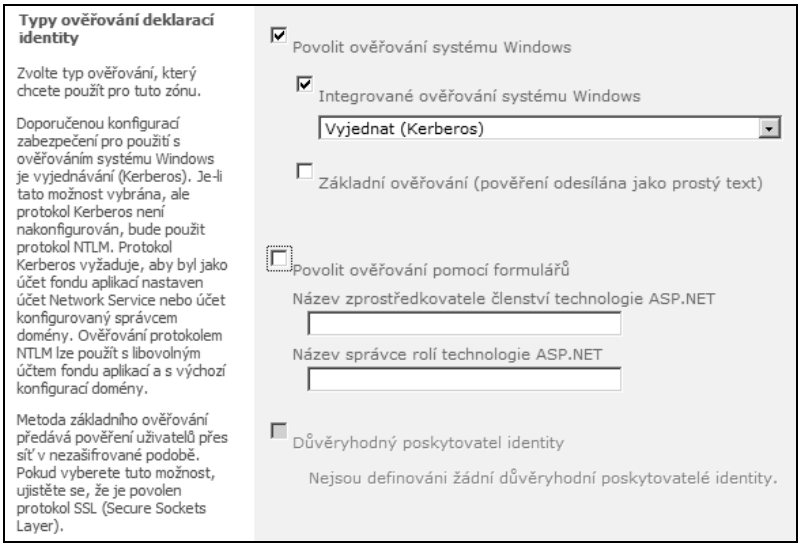
   Při výběru možnosti pro konfiguraci zabezpečení **Klasický režim ověřování** se zobrazí nastavení zachycená na obrázku 4.10.

   - **Zprostředkovatel ověřování** – pokud vytváříte intranetovou webovou aplikaci, pak řádně uvažte, zda pro autentizaci uživatelů nevyužít protokol Kerberos. Kerberos je ve srovnání s protokolem NTLM bezpečnější a nabízí lepší výkon. Máte-li více podsítí, jste-li odděleni firewally nebo pokud webová aplikace směřuje na Internet, měli byste pro autentizaci použít protokol NTLM (výchozí). Pokud uživatelé nevidí vaši službu KDC (Kerberos Distribution Center) nebo čas není synchronizovaný, autentizace pomocí protokolu Kerberos se nezdaří. Nezapomeňte při výběru protokolu Kerberos nastavit hlavní názvy služby (SPN). Informace ohledně používání a konfigurace protokolu Kerberos najdete v kapitole 15.
   - **Povolit anonymní** – pokud nenabízíte obsah pro veřejné užití, neměli byste povolit anonymní přístup. Přestože zapnutí anonymního přístupu přes danou webovou aplikaci je povoleno pro kolaborativní kolekce webů, obecně jde o špatný postup. Mějte na paměti, že samotné zapnutí anonymního přístupu pro webovou aplikaci neumožňuje anonymní přístup. Správce kolekce webů musí navíc aktivovat anonymní přístup na úrovni webu.
   - **Používat protokol SSL** – pokud vaše organizace plánuje spolupracovat přes webovou aplikaci směřující na Internet, je doporučeno zapnout kvůli bezpečnosti protokol SSL. Při zvolení protokolu SSL však musíte ve Správci služby IIS ještě přidat certifikát protokolu SSL. Tím, že zde zvolíte možnost protokolu SSL, pouze změníte schéma (*https://*) webové aplikace v konfigurační databázi, ale nesvážete certifikát s daným webem.

     Při výběru možnosti pro konfiguraci zabezpečení **Ověřování na základě deklarací identity** se zobrazí nastavení zachycená na obrázku 4.11. Poskytovatel identity obsluhuje požadavky na deklarace důvěryhodné identity jako služba IP-STS (Identity Provider Security Token Service). Služba IP-STS uchovává a spravuje identity a s nimi spojené atributy. Úložištěm identity může být tabulka v databázi SQL nebo může jít o složitější úložiště, jako je služba AD DS (Active Directory Domain Services) nebo AD LDS (Active Directory Lightweight Directory Services).
   - **Povolit ověřování systému Windows** – Výběr protokolu Kerberos nebo NTLM s deklarovaným ověřováním (**Ověřování na základě deklarací identity**) není to stejné jako v případě klasického ověřování (**Klasický režim ověřování**). Musíte mít již nakonfigurovanou službu STS (Security Token Service). Pokud chcete použít pouze autentizaci s protokolem Kerberos, základní autentizaci nebo autentizaci s protokolem NTLM, použijte klasickou

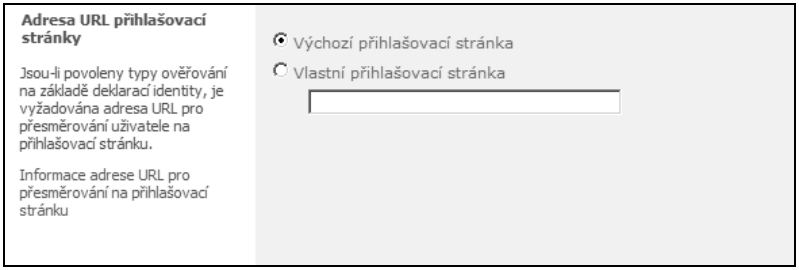
autentizaci. Při výběru základní autentizace musíte po vytvoření webové aplikace upravit poskytovatele autentizace.

- **Povolit ověřování pomocí formulářů** – zadejte název zprostředkovatele členství a název správce rolí. Tyto názvy obvykle obdržíte od svého vývojového týmu.



Obrázek 4.11: Konfigurace nastavení poskytovatele identity

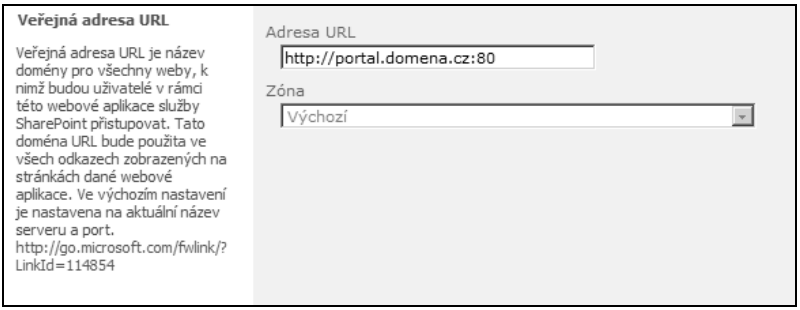
- **Důvěryhodný poskytovatel identity** – pokud používáte deklarovanou autentizaci ve federaci, zadejte příslušnou informaci do textového pole **Důvěryhodný poskytovatel identity**. Tuto informaci vám obvykle dodá váš vývojový tým.
- **Adresa URL přihlašovací stránky** – část **Adresa URL přihlašovací stránky** zachycená na obrázku 4.12 je k dispozici pouze při výběru deklarované autentizace.



Obrázek 4.12: Konfigurační nastavení v části Adresa URL přihlašovací stránky

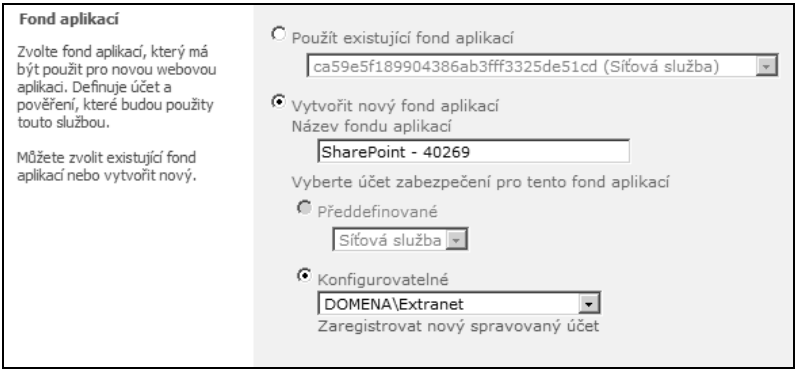
Zadání adresy URL přihlašovací stránky je nutné jen při konfiguraci autentizace na bázi formulářů. Definuje stránku zobrazenou pro zadávání přihlašovacích údajů. Samotný formulář nasadí vaši návrháři nebo vývojáři.

8. Dále zadejte veřejnou adresu URL. Veřejná adresa URL by měla být taková, kterou budou s největší pravděpodobností navštěvovat vaši uživatelé, a obvykle mívá formu plně kvalifikovaného názvu domény. Pokud jste nezvolili nestandardní port protokolu HTTP, můžete jako na obrázku 4.13 odstranit z adresy URL koncovku *:80*. Nezapomeňte upravit svůj server DNS tak, aby obsahoval údaje o nové webové aplikaci.



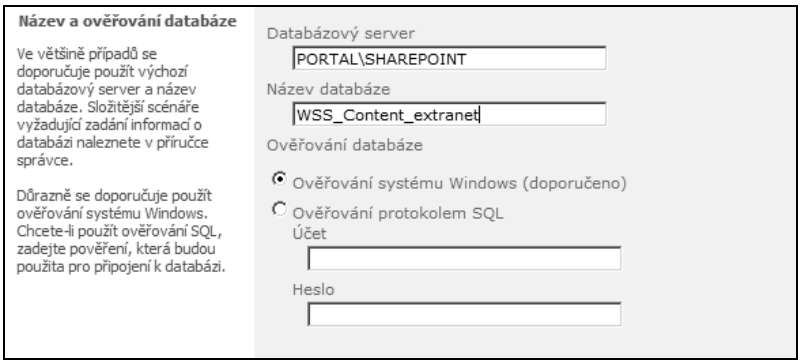
Obrázek 4.13: Konfigurační nastavení pro veřejnou adresu URL

Poznámka: Systém SharePoint Server 2010 dává uživatelům možnost rozlišovat příchozí provoz podle zón. Zóny mohou pomoci řadit příchozí provoz do různých rozšířených webových aplikací s odpovídajícími adresami URL. Adresa URL zadaná do prohlížeče uživatele se mapuje na související zónu, což umožňuje větší flexibilitu při izolování a řízení příchozího provozu. Všechny webové aplikace musí být zpočátku vytvořeny ve výchozí zóně. Podrobné informace ohledně tvorby a využívání zón najdete v kapitole 15.



Obrázek 4.14: Konfigurace nastavení pro fond aplikací

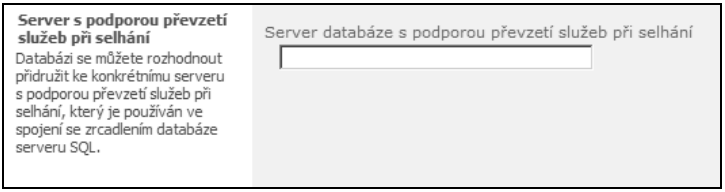
9. Rozhodněte se, zda budete používat stávající fond aplikací nebo vytvoříte nový. Je-li pro vaši organizaci důležitá bezpečnost a izolace procesů, pak musíte pro každou webovou aplikaci vytvořit fond aplikací. Vytvoření fondu aplikací vyžaduje další prostředky, jako je paměť a čas na administrativu. V 64bitovém prostředí požadovaném systémem SharePoint Server 2010 je vytvoření více fondů aplikací mnohem zajímavější, protože zde nejsou omezení paměti způsobená 32bitovým kódem. Pro vytvoření nového fondu aplikací zadejte snadno identifikovatelné jméno jako na obrázku 4.14.
10. Vyberte spravovaný účet pro identitu fondu aplikací nebo zaregistrujte nový spravovaný účet. Všimněte si, že při vytváření nového spravovaného účtu musíte na stránce znovu zadat všechny předchozí informace.
11. Dále zadejte název databázového serveru a databáze (viz obrázek 4.15).



Obrázek 4.15: Konfigurace nastavení názvu a ověřování databáze

- **Databázový server** – pro většinu instalací použijte výchozí SQL Server, který jste zadali během konfigurace farmy. Můžete vybrat jiný SQL Server (jeho instanci), máte-li několik rozsáhlých webových aplikací, které vyžadují vyhrazené, izolované obsahové databáze. Pokud používáte více instancí, zadávejte název v tomto formátu: <NÁZEV_SERVERU\instance>.
- **Název databáze** – vždy změňte výchozí název databáze tak, aby odpovídal názvu webové aplikace. Máte-li například webovou aplikaci *http://prodej.domena.cz*, použijte pro název databáze WSS_Content_Prodej. Chytré pojmenování webových aplikací, fondů aplikací a databází značně usnadňuje správu středně velkých až rozsáhlých implementací systému SharePoint Server 2010.
- **Ověřování databáze** – doporučovaným typem autentizace je autentizace systému Windows. Autentizaci SQL použijte pouze při práci v prostředí pracovní skupiny a při volbě autentizace SQL pro všechna databázová připojení včetně konfigurační databáze. Uživatel přihlášený do Centrální správy musí mít také možnost vytvářet databáze SQL Serveru.

12. Podle potřeby můžete definovat databázový server pro převzetí služeb v případě selhání. Jedná se o novou funkci systému SharePoint Server 2010 na podporu zrcadlení databáze SQL. Zrcadlení databáze SQL umožňuje databázi v případě selhání předat službu z jednoho serveru na jiný nebo na jinou instanci. Hlavní server je původní instancí a v případě jeho selhání se systém SharePoint automaticky pokouší každých 15 vteřin (výchozí nastavení) připojit k záložnímu serveru. Obsahová databáze systému SharePoint bude mít záložní databázi na záložním serveru až po konfiguraci zrcadlení SQL Serveru. Nastavení názvu záložního serveru v systému SharePoint nezajistí konfiguraci zálohy na úrovni SQL Serveru. Konfigurační část **Server databáze s podporou převzetí služeb při selhání** si můžete prohlédnout na obrázku 4.16.



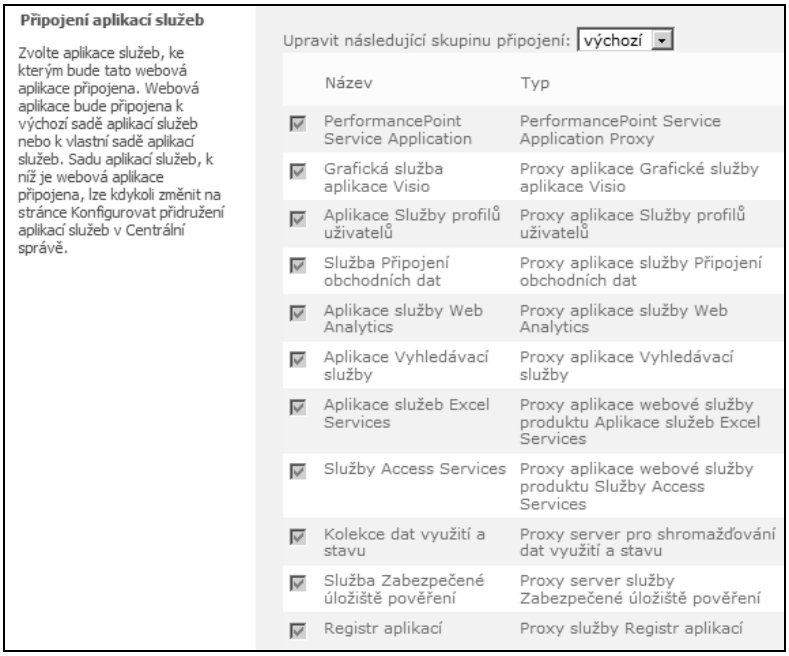
Obrázek 4.16: Nastavení Server databáze s podporou převzetí služeb při selhání

13. Podle potřeby můžete definovat vyhledávací server systému SharePoint Foundation 2010. Spojte vyhledávací server provozující službu Vyhledávání systému SharePoint Foundation 2010 s obsahovou databází, pro novou webovou aplikaci. Toto nastavení je pro vyhledávací server systému SharePoint Foundation 2010 a ne pro vyhledávací server systému SharePoint Server 2010. Je-li ve farmě nainstalovaný systém SharePoint Server 2010, pak je toto nastavení ignorováno.
14. Podle potřeby můžete změnit výchozí nastavení v části **Připojení aplikací služeb**. U většiny implementací však nebude změna nutná. Pokud máte pro servisní aplikace vlastní skupiny serverů proxy, pak musíte servisní aplikace nakonfigurovat pro tuto webovou aplikaci.

Další informace: O skupinách serverů proxy pro servisní aplikace se více dozvíte v kapitole 6.

V systému SharePoint 2007 byly služby jako Vyhledávání spravovány Zprostředkovatelem sdílených služeb. V systému SharePoint 2010 je každá služba samostatnou službou a místo nutnosti přidružení ke zprostředkovateli ji lze přidružovat nezávisle na ostatních službách. Skupina serverů proxy je podobná Zprostředkovateli sdílených služeb v tom, že ji můžete spojit s celou skupinou. V rozevírací nabídce je nastavena hodnota **[výchozí]**, která způsobí automatickou konfiguraci výběru služeb. Z této rozevírací nabídky můžete výběrem hodnoty **[vlastní]** pro webovou aplikaci nakonfigurovat připojení servisních aplikací. Tato konfigurační oblast je zachycena na obrázku 4.17.

15. Nakonec vyberte hodnotu **Ano** nebo **Ne** pro účast v programu Zlepšování softwaru a služeb na základě zkušeností uživatelů společnosti Microsoft. Přestože je dodatečná zátěž při kladné odpovědi minimální, určitý dopad mít bude.
16. Klepněte na tlačítko **OK**.



Obrázek 4.17: Konfigurace nastavení Připojení aplikací služeb

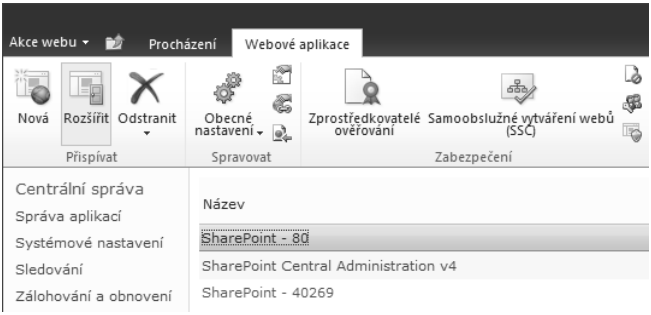
Rozšiřování webové aplikace

Díky rozšiřování webových aplikací mohou tytéž obsahové databáze nabízet obsah přes více virtuálních serverů IIS skrze tzv. *zóny*. Příkladem je organizace, která potřebuje nabízet obsah jednak interně přes *http://portal* pomocí integrované autentizace systému Windows a pak také externě přes *https://portal.domena.cz* pomocí formulářové autentizace a na protokolu SSL kvůli bezpečnosti.

Tip: Je-li nutné přistupovat k dané adrese URL interně i externě, zvažte použití nejdostupnější adresy URL jako výchozí adresy URL. Díky tomu budou k dispozici systémem generované e-mailové zprávy používající výchozí adresu URL bez ohledu na to, zda jsou interní, nebo externí. V našem příkladu je výchozí adresa URL *https://portal.domena.cz*.

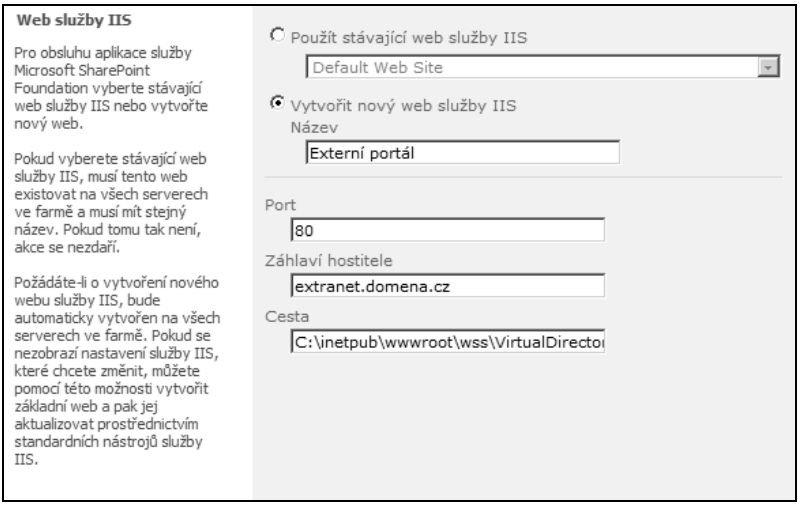
K rozšíření webové aplikace proveďte následující:

1. V Centrální správě otevřete část **Správa aplikací**, **Webové aplikace**, **Spravovat webové aplikace** a vyberte webovou aplikaci, která se má rozšířit.
2. Na pásu karet klepněte na tlačítko **Rozšířit** (viz obrázek 4.18).



Obrázek 4.18: Tlačítko Rozšířit je umístěno na pásu karet pod záložkou Webové aplikace

3. Vyberte možnost **Vytvořit nový web služby IIS**. Zadejte název, který bude ve Správci služby IIS snadno rozpoznatelný.
4. Definujte číslo portu. Pokud používáte protokol HTTP, pak se obvykle jedná o port 80. Stejně jako při vytváření webové aplikace se tato informace zapisuje do konfigurační databáze, lze ji však změnit ručně ve Správci služby IIS na každém webovém serveru farmy. Nejlepší je správně ji definovat při vytváření zóny.



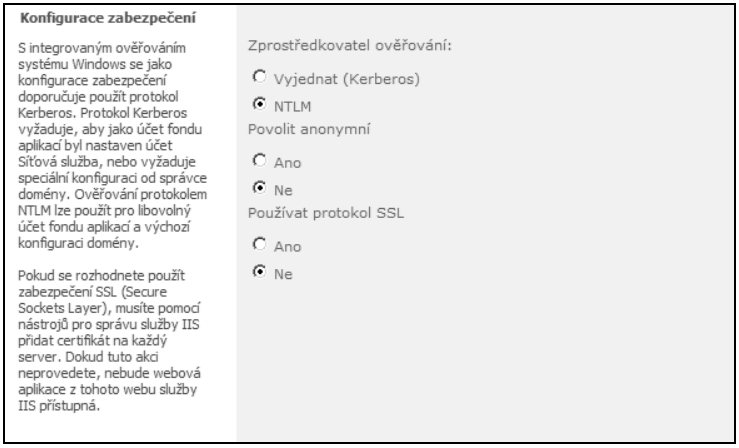
Obrázek 4.19: Pro weby služby IIS používejte vždy inteligentní jména

5. Zadejte hlavičku hostitele. Hlavička hostitele je obvykle plně kvalifikovaný název domény zóny, jako *extranet.domena.cz* na obrázku 4.19. Informaci byste měli zadat do textového pole **Záhlaví hostitele**, a to i tehdy, pokud přiřadíte IP adresy ve Správci služby IIS.

Poznámka: Pokud používáte hlavičky hostitele, změní se popis automaticky na hlavičku hostitele plus číslo portu protokolu TCP.

Tip: Pokud plánujete přiřazovat webovým aplikacím IP adresy, pak byste měli na tomto místě zadat informace o hlavičce hostitele a změnit port na 80. Vždy totiž můžete podle potřeby přidávat další hlavičky hostitele ve Správci služby IIS. Tím se proces přidávání dalších webových front-end (WFE) serverů do farmy zjednoduší.

6. Dále se rozhodněte, zda budete používat protokol NTLM, Kerberos, nebo základní autentizaci. Potřebujete-li používat základní autentizaci, vyberte protokol NTLM a po dokončení rozšiřování webové aplikace nakonfigurujte poskytovatele autentizace. Pokud používáte Kerberos, nezapomeňte registrovat hlavní název služby (SPN) pro identitu fondu webových aplikací výchozí zóny. Konfigurace možností zabezpečení je zachycena na obrázku 4.20.



Obrázek 4.20: Rozšíření konfigurace zabezpečení webové aplikace

Další informace: Více informací o konfiguraci hlavního názvu služby protokolu Kerberos pro doménový účet uživatele najdete v kapitole 15.

Upozornění: Nemáte možnost vytvořit další fond webových aplikací. Tím by se totiž narušila funkčnost rozšíření webové aplikace. Proto nikdy ve Správci služby IIS neměňte fond aplikací rozšířeného webu.

7. Pokud rozšiřujete konfiguraci o využití zabezpečení ve formě protokolu SSL, nezapomeňte zde tuto možnost zvolit. I když toto nastavení můžete změnit i později, snazší je provést to nyní. Všimněte si, že po vytvoření je před úspěšným interpretováním obsahu přes protokol SSL ještě zapotřebí ve Správci služby IIS nakonfigurovat certifikát pro tento web. Systém SharePoint Server 2010 totiž neprovádí svazování certifikátu s webem služby IIS.

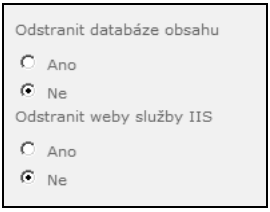
Poznámka: Certifikáty protokolu SSL a přiřazené IP adresy se neukládají do konfigurační databáze. Pokud musíte z nějakého důvodu webový server obnovit, budete muset webové aplikace používající protokol SSL nebo přiřazené IP adresy znovu nakonfigurovat. Další možností je obnovení služby IIS z poslední zálohy.

8. Dále definujte veřejnou adresu URL. Tuto adresu URL lze nastavit na dříve definovaný název hostitele služby DNS (Domain Name System) pro tuto webovou aplikaci nebo na název hostitele DNS pro IP adresu pro službu Vyrovnávání zatížení sítě (Network Load Balancing). V systému SharePoint 2007 se tato adresa jmenovala adresa URL s vyrovnáváním zatížení sítě (Load Balanced URL).
9. Vyberte zónu.
10. Klepněte na tlačítko **OK**.

Odstranění webové aplikace

Při mazání webové aplikace byste si měli počínat velmi obezřetně. Před vymazáním webové aplikace vždy zkontrolujte, zda máte zálohu farmy. K vymazání webové aplikace proveďte následující:

1. V Centrální správě otevřete **Správu aplikací**, **Spravovat webové aplikace**.
2. Vyberte webovou aplikaci, kterou chcete vymazat, a na pásu karet klepněte na tlačítko **Odstranit**.
3. Chcete-li vymazat obsahové databáze, zvolte možnost **Ano**. V opačném případě ponechejte výchozí nastavení jako na obrázku 4.21.



Obrázek 4.21: Možnosti dostupné při mazání webové aplikace

4. Pro vymazání webu služby IIS vyberte možnost **Ano**. Je možné vymazat definici webové aplikace v konfigurační databázi a přitom ponechat obsahovou databázi či databáze a web služby IIS beze změn.

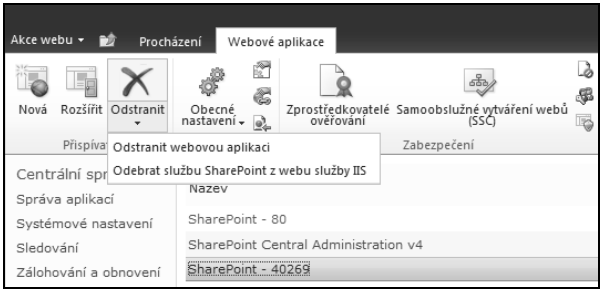
5. Klepněte na tlačítko **Odstranit**.

K odebrání rozšířené webové aplikace ze služby IIS postupujte podle těchto kroků:

1. V Centrální správě otevřete část **Správa aplikací**, **Webové aplikace**, **Spravovat webové aplikace**.
2. Vyberte webovou aplikaci, kterou chcete vymazat.
3. Na pásu karet zobrazte klepnutím na šipku dolů rozevírací nabídku pro tlačítko **Odstranit** a vyberte příkaz **Odstranit webovou aplikaci** (umístění na pásu karet zachycuje obrázek 4.7).
4. Chcete-li vymazat obsahové databáze, zvolte možnost **Ano**.
5. Vyberte možnost **Ano** pro vymazání všech webů služby IIS, jež byly vytvořeny pro webovou aplikaci a které tato webová aplikace zároveň používala.
6. Klepněte na tlačítko **Odstranit**.

Odebrání služby SharePoint z webu služby IIS

Odebrání služby SharePoint z webu služby IIS je podobné, jako odstranění webové aplikace, ovšem s tím rozdílem, že můžete vybrat weby služby IIS spojené s danou zónou, ne však obsahovou databázi. Rozhodnete-li se odebrat systém SharePoint ze stávajícího webu služby IIS, buďte při výběru možnosti na pásu karet velice obezřetní. Neklepejte na tlačítko **Odstranit**, které představuje primární možnost pro vymazání, ale klepněte na tlačítku **Odstranit** na šipku dolů a vyberte možnost **Odebrat služby SharePoint z webu služby IIS** (viz obrázek 4.22).



Obrázek 4.22: Vymažte webovou aplikaci nebo ji odeberte ze služby IIS

K odebrání služby SharePoint z webu služby IIS proveďte následující:

1. V Centrální správě otevřete **Správu aplikací**, **Spravovat webové aplikace**.
2. Vyberte webovou aplikaci s přidruženou zónou, kterou chcete vymazat. Obrázek 4.18 ukazuje příklad výběru webové aplikace.
3. Klepnutím na šipku dolů umístěnou na pásu karet na tlačítku **Odstranit** zobrazte rozevírací nabídku a vyberte příkaz **Odebrat službu SharePoint z webu služby IIS**.

4. Klepnutím na šipku dolů zobrazte rozevírací nabídku **Vybrat web služby IIS a zónu k odebrání**.
5. Klepněte na možnost **Ano** a poté na tlačítko **OK**.

Důležité: Při mazání či odebírání systému SharePoint z webu služby IIS dávejte velký pozor. Zobrazí se výchozí zóna, avšak smazány budou všechny zóny přidružené k webové aplikaci.

Správa webových aplikací

Systém SharePoint Server 2010 má pro všechna nastavení související se správou aplikací nové rozhraní s pásem karet. Většinu běžných činností lze provádět prostřednictvím správcovského pásu karet, který se objeví v Centrální správě po otevření **Správy aplikací**, **Spravovat webové aplikace**. Při výběru webové aplikace se tento pás karet změní a zobrazí relevantní konfigurační možnosti. Rozhraní s pásem karet je rozděleno na následující oblasti:

- Přispívat
- Spravovat
- Zabezpečení
- Zásady

Kromě toho potřebujete spravovat alternativní mapování adres URL, k němuž se dostanete tak, že v Centrální správě otevřete **Správu aplikací**, **Konfigurovat mapování alternativních adres URL**. Jedná se o stejná nastavení alternativního mapování adres URL jako v části **Zabezpečení**.

Konfigurace webových aplikací

Po vytvoření webové aplikace je potřeba dokončit mnoho dalších činností. Proces tvorby webové aplikace se postará jen o minimální požadavky na definování webové aplikace v konfigurační databázi, což zahrnuje konfiguraci služby IIS a vytvoření první přidružené obsahové databáze.

Pro správu obsahové databáze musíte na pásu karet otevřít záložku **Webové aplikace**. V příkladu zobrazeném na obrázku 4.23 je webovou aplikací vybranou ke konfiguraci aplikace SharePoint – 80.

Každá webová aplikace má jednotlivá nastavení, která mají vliv na všechny weby a kolekce webů, pro něž je daná webová aplikace hostitelem. Obrázek 4.24 zachycuje rozbalenou nabídku **Obecné nastavení**, která obsahuje jiné možnosti než ty, jež jsou obsaženy v hlavní záložce **Obecné nastavení**.