Windows Server 2008

Active Directory

Kapesní rádce administrátora

William R. Stanek

- Nástroje, techniky a koncepty Active Directory
- Instalace doménových struktur, stromů domén a podřízených domén
- Údržba, sledování a řešení problémů s Active Directory
- Konfigurace a správa serverů globálního katalogu
- Všechny nástroje příkazového řádku služby Active Directory

CPRESS

Microsoft

William R. Stanek

Active Directory
Kapesní rádce administrátora

Computer Press, a. s.
Brno
2009

Active Directory
Kapesní rádce administrátora

William R. Stanek

Computer Press, a. s., 2009. Vydání první.

Překlad: Michaela Vaidová, Pavel Vaida
Odborná korektura: Martin Ivaniš
Jazyková korektura: Pavel Bubla
Vnitřní úprava: Martin Hubík
Sazba: Martin Hubík
Rejstřík: Daniel Štreit
Obálka: Martin Sodomka

Komentář na zadní straně obálky: Libor Pácl
Technická spolupráce: Jiří Matoušek, Zuzana Šindlerová, Dagmar Hajdajová
Odpovědný redaktor: Libor Pácl
Technický redaktor: Jiří Matoušek
Produkce: Petr Baláš

Computer Press, a. s.,
Holandská 8, 639 00 Brno

Objednávky knih:
http://knihy.cpress.cz
distribuce@cpress.cz
tel.: 800 555 513

ISBN 978-80-251-2555-7
Prodejní kód: K1711
Vydalo nakladatelství Computer Press, a. s., jako svou 3347. publikaci.

Stručný obsah

Obsah

O autorovi

William R. Stanek (*http://www.williamstanek.com/*) se narodil v Burlingtonu ve státě Wisconsin, USA, kde navštěvoval veřejné školy, včetně Janes Elementary School ve městě Racine, Wisconsin. Je druhým nejmladším z pěti dětí. Po skončení služby v armádě se usadil ve státě Washington, kde jej uchvátila drsná krása pacifického severozápadu.

V roce 1985 narukoval k americkému letectvu a nastoupil dvouletý výukový program ve zpravodajské činnosti a lingvistice u Defense Language Institute. Po absolvování sloužil v různých operacích v Asii a Evropě. V roce 1990 získal místo na škole Air Combat School a krátce po absolvování sloužil ve válce v Perském zálivu jako člen zásahového komanda v divizi pro elektronický boj u vojenského letectva. Během svých dvou misí ve válce v Perském zálivu se William účastnil několika vzdušných misí a bojových podpůrných misí, čítaje přes 200 bojových letových hodin. Za své vynikající úspěchy během války byl oceněn devíti vyznamenáními, včetně nejvyšší letecké pocty USA, Záslužného leteckého kříže vzdušných sil (Air Force Distinguished Flying Cross), stejně jako letecké vyznamenání (Air Medal), medaili vzdušných sil za zásluhy (Air Force Commendation Medal) a medaili za humanitární službu (Humanitarian Service Medal). Za svou vojenskou kariéru získal 29 vyznamenání.

V roce 1994 byl Williamovi udělen bakalářský titul s vyznamenáním od Hawaii Pacific University. V roce 1995 mu byl udělen magisterský titul s vyznamenáním od Hawaii Pacific University. V roce 1996 odešel pod odsloužení 11 let u amerického letectva od armády. Během své služby v armádě sloužil v Texasu, Japonsku, Německu a na Havaji. Sloužil u podpůrné jednotky operace Pouštní bouře, operace Pouštní štít a operace Provide Comfort. Jeho posledním působištěm u vzdušných sil byla 324. zpravodajská eskadra vojenského letiště Wheeler na Havaji.

William se narodil v rodině, v níž se hodně četlo, takže i on rád četl a psal příběhy. Ještě před nástupem do školy četl klasickou literaturu jako *Ostrov pokladů*, *Švýcarský Robinzon*, *Robinson Crusoe* a *Tři mušketýři*. Později jako dítě začal číst díla autorů jako byli Jules Verne, Sir Arthur Conan Doyle, Edgar Rice Burroughs, Ray Bradbury, Herman Melville, Jack London, Charles Dickens a Edgar Allan Poe. K tomu William dodává: „Edgar Allan Poe dokáže být pěkně drsný a zlověstný, zejména když je vám deset. Ale vzpomínám si, že mě jeho příběhy fascinovaly. Dodnes si pamatuji na úryvky jeho děl ‚*Havran*' ‚‚*Zrádné srdce*' a, *Vraždy v Rue Morgue*"".

William dokončil svůj první román v roce 1986, když byl převelen do Japonska, ale trvalo téměř deset let, než byla jeho první kniha vydána. Od té doby napsal a vydal téměř 100 knih, včetně *Active Directory Kapesní rádce administrátora*, *Windows Server 2008 Kapesní rádce administrátora*, *Microsoft SQL Server 2008 Administrator's Pocket Consul-*

tant a *Mistrovství v Microsoft Windows Server 2008* (všechny od vydavatelství Microsoft Press, tři z nich přeloženy nakladatelstvím Computer Press).

V roce 1997 měl William přezdívku „tvář budoucnosti" v článku o jeho životě v deníku The (Wash.) *Olympian*. V té době vytvářel podmínky pro budoucí internetové podnikání. Dnes William nadále pomáhá formovat budoucnost internetového podnikání a technologií obecně – píše spolehlivé knihy týkající se těchto témat pro mnoho vydavatelů. William získal od svých kolegů a vydavatelské branže mnohá ocenění.

Ve svém volném čase trávil hodně času jízdou na horském kole a turistikou, ovšem dnes jsou jeho dobrodružství v nádherné přírodě téměř omezena jen na krátké výlety po pacifickém severozápadu. V roce 2009 bude společností Microsoft vydána Williamova stá kniha. Williamovo celoživotní odevzdání se psanému slovu mu pomohlo stát se jedním z dnešních nejuznávanějších světových autorů píšících o technologiích.

Poděkování

Když píšete knihy už delší dobu, lidé se vás ptají, kolik knih jste už napsali, a vy nemáte ani ponětí. Mnoho let jsem ve svém životopise uváděl, že jsem autorem více než 25 knih. Několikrát mě mí vydavatelé požádali, abych svůj životopis aktualizoval přesnějším číslem, takže ke vší spokojenosti jsem se dopočítal k číslu 61. Tedy to bylo asi před pěti, šesti, sedmi lety, takže dnes se blížím k číslu 100 nebo tak nějak. ;-)

Umění psát pro mě vždy hodně znamenalo. Miluji psaní a ze všeho nejvíce miluji projekty, které jsou pro mě výzvou. S výzvou napsat průvodce pro každodenní administraci služby Active Directory je spojeno mnoho témat, o nichž bych se rád zmínil, ovšem kapesní rádci nejsou referenčními příručkami, v nichž naleznete vše. Kapesní rádci mají být příruční a srozumitelní – tedy má jít o takový druh knihy, kterou použijete k řešení problémů a zvládnutí úkolů za všech okolností. Maje tyto aspekty na paměti, zaměřil jsem se na klíčové úlohy správy služby Active Directory. Výsledkem je kniha, kterou právě držíte v rukou, a jež pro vás – doufám – bude jedním z nejpraktičtějších, kapesních průvodců ke službě Active Directory.

Jak jsem uvedl v přibližně čtyřiceti kapesních rádcích, které jsem již napsal, tým nakladatelství Microsoft Press je bezvadný. Po celou dobu psaní mi byla nápomocná Maria Gargiulová. Pomohla zajistit vše, co jsem potřeboval k psaní knihy, a byla mým primárním kontaktem ve společnosti Microsoft. Martin DelRe byl akvizičním redaktorem celého projektu. Věřil v knihu od začátku a byla skutečně radost s ním pracovat. Kompletace a vydání knihy by byly bez jejich pomoci nemožné!

Bohužel pro autora (ale naštěstí pro čtenáře), psaní je pouze jednou částí vydavatelského procesu. Následuje úprava textu a odborná recenze. Musím říci, že vydavatelství Microsoft Press má zvládnut nejpropracovanější editorský a korektorský proces, který jsem kdy viděl – a to jsem napsal spoustu knih pro mnohá různá nakladatelství. Redakční proces řídil John Pierce. Pomohl mi držet se tématu a harmonogramu. Randy Muller byl technickým redaktorem knihy. Shannon Leavitt, coby pomocný redaktor, rovněž odvedl skvělou práci. Díky vám všem!

Rád bych poděkoval Chrisi Nelsonovi za jeho pomoc při realizaci celého projektu. Spolupráce s Chrisem je úžasná, vždy chce pomoci, jakkoliv je potřeba. Díky rovněž všem ve společnosti Microsoft, kteří mi mnohokrát pomohli v mé spisovatelské kariéře a byli mi k dispozici vždy, když jsem je nejvíc potřeboval.

Dík patří také agentuře The Salkind Agency společnosti Studio B a mému agentovi Neilovi Salkindovi.

Doufám, že jsem nezapomněl na nikoho, ale pokud ano, bylo to jen nedopatřením. *Opravdu*.

Úvod

Kniha *Active Directory Kapesní rádce administrátora* je navržena tak, aby byla stručným a použitelným zdrojem pro správce systému Windows. Jde tedy o čtivého průvodce, kterého vždy budete chtít mít na svém stole nebo ve své kapse. Tato kniha popisuje všechno, co je třeba k provedení hlavních úloh správy služby Active Directory. Jelikož důraz je kladen na maximální přínos tohoto průvodce kapesní velikosti, nebudete se muset prokousávat stovkami stran nesouvisejících informací, abyste zjistili to, co hledáte. Místo toho najdete přesně to, co potřebujete vědět k tomu, abyste mohli dobře odvést svou práci.

Stručně řečeno, tato kniha má být jediným zdrojem, do kterého nahlédnete vždy, když budete mít nějaké otázky týkající se správy služby Active Directory. Proto se tato kniha zaměřuje na každodenní procedury týkající se správy, na často prováděné úlohy, dokumentované příklady a možnosti, které jsou názorné, ale ne nezbytně kompletní. Jedním z cílů je dodržet takovou stručnost, aby byla kniha kompaktní a usnadňovala snadnou navigaci, ale aby současně obsahovala co možná nejvíce informací – a byla tak cenným zdrojem. Proto se k vám místo statné tisícistránkové bichle či lehké stostránkové referenční příručky dostává cenný průvodce, který vám pomůže efektivně provádět běžné úlohy, řešit problémy a implementovat i tak pokročilé oblasti správy jako je vytváření vztahů důvěryhodnosti mezi doménovými strukturami, optimalizace replikace mezi lokalitami, změna návrhu domény a řešení problémů.

Komu je tato kniha určena?

Kniha *Active Directory Kapesní rádce administrátora* pokrývá službu Active Directory pro malé, střední a velké organizace. Tato kniha je určena pro:

- stávající správce systému Windows a správce sítí;
- zaměstnance podpory, kteří udržují sítě Windows;
- kvalifikované uživatele, kteří mají určité administrátorské povinnosti;
- správce přecházející z jiných platforem.

Abych zde napěchoval co nejvíce možných informací, musel jsem předpokládat, že máte základní znalosti o sítích a platformě Windows, a že na svých počítačích již máte nainstalován systém Windows. S tímto požadavkem na paměti nevěnuji celé kapitoly pochopení architektury systému Windows, instalaci systému Windows nebo vytváření sítí na platformě Windows. Ovšem uvádím veškeré podrobnosti o součástech sítí se službou Active Directory a o tom, jak můžete tyto součásti použít. Zmiňuji se o instalaci řadičů domény, konfiguraci lokalit služby Active Directory a mnohém dalším.

Rovněž předpokládám, že jste relativně dobře obeznámeni s příkazy a procedurami systému Windows, stejně jako s uživatelským rozhraním systému Windows. Pokud se potřebujete naučit základy týkající se systému Windows, měli byste si přečíst dokumentaci k tomuto systému.

Jak je kniha uspořádána?

Kniha *Active Directory Kapesní rádce administrátora* je navržena pro použití při každodenní správě služby Active Directory, a jako taková je celá kniha uspořádána podle jednotlivých úloh, místo podle funkcí. Rychlost a snadnost odkazování jsou důležitými aspekty tohoto příručního průvodce. Tato kniha obsahuje rozšířený obsah a rozsáhlý rejstřík pro rychlé vyhledání odpovědí na vaše otázky. Přidána byla také spousta jiných funkcí pro rychlé odkazování. Patří mezi ně rychlé pokyny krok za krokem, seznamy, tabulky s rychlými fakty a spousta křížových odkazů. Tato kniha je uspořádána na části i kapitoly.

Služba Active Directory je rozšířitelná adresářová služba, která vám umožní efektivně spravovat síťové prostředky. Část I, „Implementace služby Active Directory", se týká základních úloh, které jsou potřebné ke správě služby Active Directory. Kapitola 1 obsahuje přehled nástrojů, technik a konceptů týkajících se služby Active Directory. Kapitola 2 popisuje instalaci doménových struktur, stromů domén a podřízených domén. V kapitole 1 a 2 jsou rovněž popsány aktualizace služby Active Directory pro systém Windows Server 2008 Release 2 (R2). Kapitola 3 se zabývá technikami nasazení řadičů domén s možností zápisu a úlohami potřebnými k nastavení řadičů domény. Kapitola 4 se zabývá nasazením řadičů domén jen pro čtení. Společně tyto kapitoly podávají podrobné informace potřebné ke konfiguraci domén a doménových struktur, ať už nasazujete službu Active Directory Domain Services poprvé, nebo rozšiřujete vaši stávající infrastrukturu.

Část II, „Správa infrastruktury služby Active Directory", se týká základních nástrojů a technik, které použijete ke správě služby Active Directory. Kromě svých běžných rolí mohou řadiče domény fungovat také jako servery globálního katalogu a hlavní operační servery. Kapitola 5 analyzuje techniky konfigurace a správy serverů globálního katalogu a řešení problémů s nimi souvisejících. Kapitola 6 se zabývá způsobem správy hlavních operačních serverů. Kapitola 7 vám popisuje práci s lokalitami, podsítěmi a replikacemi služby Active Directory. Naučíte se základy vytváření lokalit a asociace podsítí s lokalitami. Rovněž se dozvíte o pokročilých technikách správy propojení lokalit a replikací.

Část III, „Údržba a obnova služby Active Directory", se týká úloh správy, které budete používat při údržbě služby Active Directory. Kapitola 8 popisuje způsoby správy vztahů důvěryhodnosti a ověřování. Dozvíte se o tom, jak funguje ověřování služby Active Directory v rámci domén, za hranice domén a za hranice doménových struktur. Také se naučíte, jak se vztahy důvěryhodnosti používají a vytvářejí. Kapitola 9 se zmiňuje o technikách, které můžete použít pro údržbu, sledování a řešení problémů s infra-

strukturou služby Active Directory. Kromě toho, že se dozvíte o technikách zálohování a obnovení služby Active Directory, naučíte se také to, jak provádět základní úlohy údržby a jak konfigurovat související možnosti a služby, včetně služby Systémový čas (Windows Time).

A konečně Příloha A obsahuje stručnou referenční příručku nástrojů příkazového řádku, které použijete při práci se službou Active Directory.

Konvence použité v knize

Pro lepší srozumitelnost a jednoduchost textu jsem použil různé prvky. Najdete zde výpisy kódu a seznamy psané písmem se stejnou roztečí, kromě případů, kdy vám řeknu, abyste skutečně zadali určitý příkaz. V takovém případě bude příkaz vysázen **tučným** písmem. Při zavedení a definici nového výrazu jej zvýrazním *kurzívou*.

Další použité konvence:

Poznámky – obsahují informace o určitém tématu, které vyžaduje zdůraznění.

Doporučené postupy – pro vyzkoušení doporučeného postupu, který se má použít při práci s pokročilými koncepty konfigurace a správy.

Upozornění – pro vaše upozornění na možné problémy, na které byste si měli dát pozor.

Z praxe – obsahuje praktickou radu k pokročilým tématům.

Bezpečnostní upozornění – zdůrazňuje důležitou problematiku týkající se zabezpečení.

Tipy – nabízí užitečné rady nebo další informace.

Upřímně doufám, že v této knize *Active Directory Kapesní rádce administrátora* najdete všechno, co budete potřebovat k provádění základních úloh správy služby Active Directory co možná nejrychleji a nejefektivněji. Vaše náměty jsou vítány na mé adrese *williamstanek@aol.com*. Děkuji vám.

Další obsah naleznete na Internetu

Nové nebo aktualizované materiály, doplňující tuto knihu, se budou objevovat na webových stránkách Microsoft Press Online Windows Server and Client Web. Mezi materiály, které zde můžete najít, patří aktualizovaný obsah knihy, články, odkazy na doplňující obsah, errata, vzorové kapitoly a mnohé další. Tyto webové stránky jsou dostupné

na adrese *www.microsoft.com/learning/books/online/serverclient* a jsou pravidelně aktualizovány.

Podpora

Přesnosti této knihy bylo věnováno veškeré úsilí. Vydavatelství Microsoft Press zveřejňuje opravy ke knihám prostřednictvím webových stránek na následující adrese:

http://www.microsoft.com/mspress/support

Máte-li jakékoliv komentáře, dotazy nebo náměty týkající se této knihy, prosíme, pošlete je vydavatelství Microsoft Press, a to některým z níže uvedených způsobů:

Poštou:

Microsoft Press
Attn: Editor, *Active Directory Administrator's Pocket Consultant*
One Microsoft Way
Redmond, WA 98052-6399

E-mail:

mspinput@microsoft.com

Prosíme, vezměte na vědomí, že prostřednictvím těchto adres není nabízena podpora k produktu. Informace o podpoře naleznete na webových stránkách společnosti Microsoft na adrese *http://support.microsoft.com*.

Poznámka redakce českého vydání

I nakladatelství Computer Press, které pro vás tuto knihu přeložilo, stojí o zpětnou vazbu a bude na vaše podněty a dotazy reagovat. Můžete se obrátit na následující adresy:

Computer Press
redakce počítačové literatury
Holandská 8
639 00 Brno
nebo
knihy@cpress.cz.

Další informace a případné opravy českého vydání knihy najdete na internetové adrese *http://knihy.cpress.cz/K1711*. Prostřednictvím uvedené adresy můžete též naší redakci zaslat komentář nebo dotaz týkající se knihy. Na vaše reakce se srdečně těšíme.

ČÁST I

Implementace služby Active Directory

KAPITOLA 1

Přehled služby Active Directory

V této kapitole:

Ať už jste zkušený správce, který pracoval se sítěmi systému Windows už léta, nebo nováček se základními znalostmi, váš dlouhodobý úspěch v oblasti neustále se měnících technologií do značné míry závisí na tom, jak dobře porozumíte službě Active Directory. *Active Directory* je rozšiřitelná adresářová služba, která umožňuje centralizovanou správu síťových prostředků. Umožní vám snadno přidávat, odebírat nebo přemisťovat účty pro uživatele, skupiny a počítače, stejně jako jiné typy prostředků. Téměř každá úloha správy, kterou provedete, nějakým způsobem souvisí se službou Active Directory. Služba Active Directory je založena na standardních internetových protokolech a její návrh vám pomůže jasně identifikovat fyzické a logické součásti struktury vaší sítě.

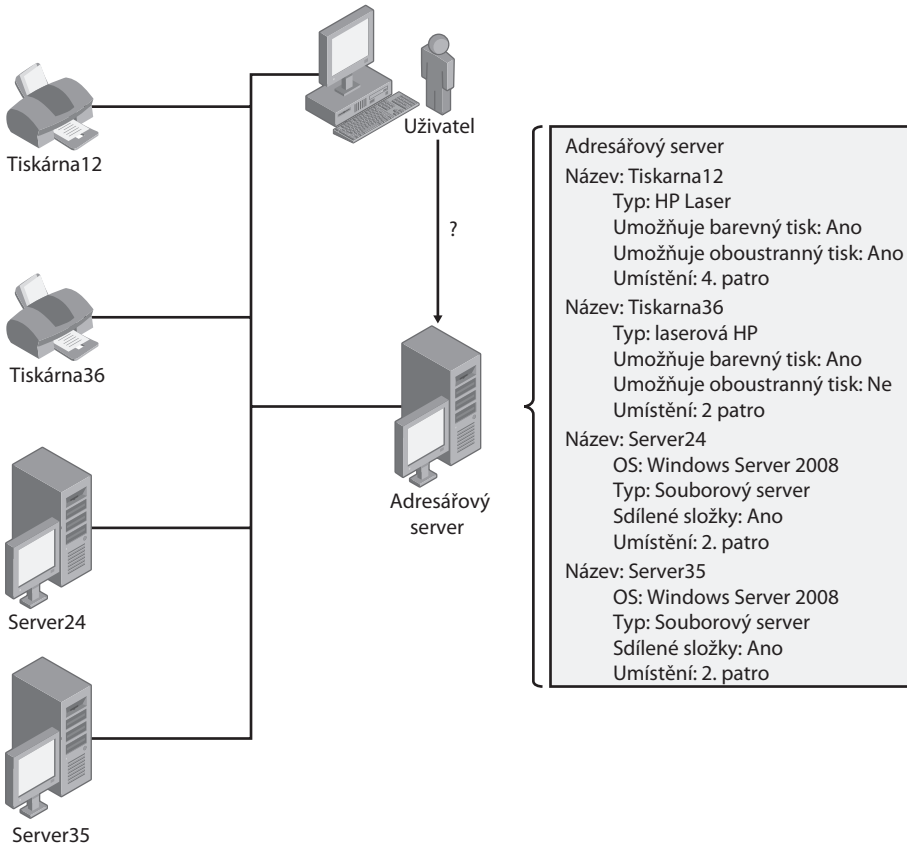
Pochopení adresářových služeb

Služba Active Directory poskytuje nezbytnou infrastrukturu pro vytváření adresáře, který plní potřeby vaší organizace. *Adresář* je uloženou kolekcí informací o různých typech prostředků. V distribuovaném výpočetním prostředí, jakým je například síť se systémem Windows, musí být uživatelé schopni najít a používat distribuované prostředky a správci musí být schopni spravovat způsob použití těchto distribuovaných prostředků. Proto je adresářová služba nezbytností.

Adresářová služba ukládá veškeré informace potřebné k použití a správě distribuovaných prostředků na jednom místě. Tato služba umožňuje spolupráci těchto prostředků. Je zodpovědná za ověření přístupu, správu identit a kontrolu vztahů mezi prostředky. Jelikož adresářová služba poskytuje tyto základní funkce, musí být úzce svázána s bezpečnostními funkcemi síťového operačního systému a s jeho funkcemi pro správu.

Adresářová služba poskytuje prostředky k definici a údržbě síťové infrastruktury, provádění správy systému a kontrole prostředí pro uživatele. Ačkoliv uživatelé a správci nemusí znát přesné prostředky, jež potřebují, měli by znát některé základní charakte-

ristické vlastnosti prostředků, jež chtějí použít. V takovém případě mohou použít adresářovou službu k zobrazení seznamu prostředků, odpovídajících jejich požadavkům. Jak můžete vidět na obrázku 1.1, uživatelé mohou použít adresářovou službu k zjištění adresáře a nalezení prostředků s konkrétními vlastnostmi. Uživatelé mohou v adresáři vyhledat například barevnou tiskárnu na určitém konkrétním místě nebo najít barevnou tiskárnu, která umožňuje oboustranný tisk.



Obrázek 1.1: Práce s adresářovými službami

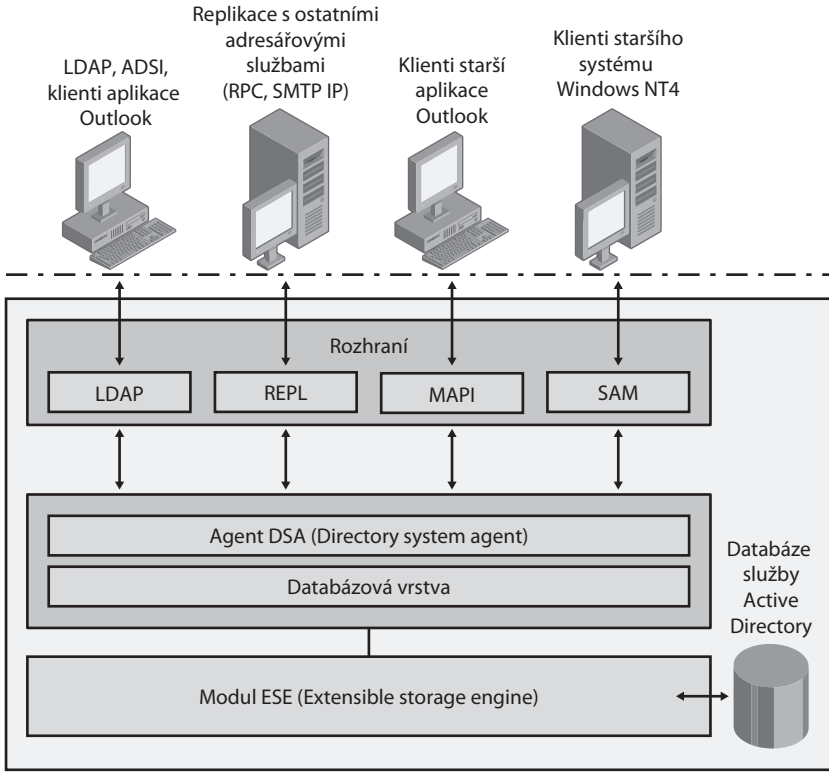
Jelikož adresářová služba je nástrojem pro správce i běžné uživatele, správci mohou používat adresář také k vyhledávání prostředků. Správce by mohl například vyhledat souborové servery s operačním systémem Windows Server 2008. S růstem organizace i její sítě přibývá stále více prostředků, které je třeba spravovat, a adresářová služba se stává stále důležitější.

Úvod do služby Active Directory

Active Directory je adresářová služba obsažená v systému Windows Server. Active Directory zahrnuje adresář, v němž jsou uloženy informace o vašich distribuovaných prostředcích, stejně jako o službách, díky nimž jsou tyto informace užitečné a dostupné. Všechny verze systému Windows Server od systému Windows 2000 podporují Active Directory.

Domény služby Active Directory

Domény systému Windows, které používají službu Active Directory, se nazývají *domény služby Active Directory*. V doméně služby Active Directory jsou vaše data uložena v jediném, distribuovaném úložišti dat, jehož údržba vyžaduje menší rozsah správy při současném umožnění snadného přístupu ze všech umístění v síti. S využitím fyzických a logických struktur poskytovaných službou Active Directory můžete měnit velikost ad-



Obrázek 1.2: Služba Active Directory umí spolupracovat s klienty a jinými adresářovými službami

resáře tak, aby splňoval vaše obchodní a síťové požadavky, ať už máte stovky, tisíce či miliony prostředků.

Služba Active Directory je navržena tak, aby vzájemně spolupracovala s dalšími adresářovými službami a aby akceptovala požadavky od mnoha různých klientů, využívajících různá rozhraní (viz obrázek 1.2). Primárním protokolem, který služba Active Directory používá, je protokol LDAP verze 3 (Lightweight Directory Access Protocol), což je standardní protokol pro adresářové služby. Při práci s jinými servery se systémem Windows služba Active Directory podporuje replikaci prostřednictvím rozhraní REPL. Při práci se staršími klienty zasílání zpráv služba Active Directory podporuje rozhraní MAPI (Messaging Application Programming Interface). Služba Active Directory rovněž podporuje rozhraní SAM (Security Accounts Manager).

Autentizační a autorizační služby Active Directory implicitně používají k zajištění ochrany dat při současné maximalizaci flexibility protokol Kerberos verze 5 a další standardní protokoly. Služba Active Directory například standardně podepisuje a šifruje veškerou komunikaci, která používá protokol LDAP. Podepisování komunikace protokolu LDAP zaručuje, že data pochází ze známého zdroje a nebyla změněna.

Služba Active Directory je integrována do zabezpečení serveru Windows Server. Pomocí podrobné množiny oprávnění můžete řídit přístup k distribuovaným prostředkům v adresáři, podobně jako je tomu u souborů a složek. Také můžete řídit přístup k vlastnostem distribuovaných prostředků. Kromě toho, služba Active Directory nabízí skupiny zabezpečení pro správu na různých úrovních v celé rozlehlé síti.

Zásady zabezpečení ve službě Active Directory se používají k definování povolených akcí a nastavení pro uživatele a počítače. Administrace založená na zásadách zjednodušuje mnoho úloh správy. Zásady skupiny lze použít mnoha různými způsoby. Jedním z nich je použít šablony zabezpečení ke konfiguraci počátečního zabezpečení počítače.

Domény DNS

Služba Active Directory používá službu DNS (Domain Name System). Služba DNS je standardní internetovou službou, která organizuje skupiny do hierarchické struktury. Třebaže jsou implementovány z různých důvodů, služby Active Directory a DNS mají stejnou hierarchickou strukturu. Hierarchie služby DNS je pro veřejné sítě definována na úrovni Internetu a pro privátní sítě na úrovni organizací. Různé úrovně v hierarchii služby DNS identifikují jednotlivé počítače a vztahy mezi počítači. Vztah mezi počítači je vyjádřen pomocí domén. Počítače, které jsou součástí stejné domény DNS, jsou blízce příbuzné. Domény použité v organizacích jsou *organizačními doménami*. Domény při kořeni hierarchie služby DNS jsou *doménami nejvyšší úrovně*, též kořenovými doménami.

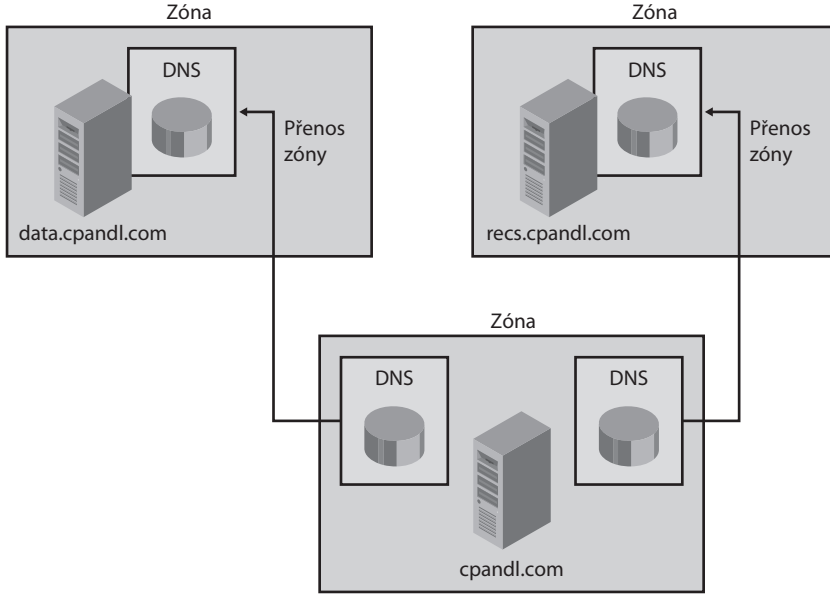
Klienti služby Active Directory používají službu DNS k nalezení prostředků. Služba DNS překládá snadno čitelné názvy hostitelů na číselné adresy protokolu IP (Internet Protocol). Každému počítači v doméně je přiřazen plně kvalifikovaný název domény (FQDN), například server34.microsoft.com. V tomto případě *server34* je názvem jed-

notlivého počítače, *microsoft* vyjadřuje organizační doménu a *com* je doménou nejvyšší úrovně.

Domény nejvyšší úrovně tvoří základ hierarchie služby DNS. Domény nejvyšší úrovně jsou uspořádány geograficky použitím dvoupísmenných kódů zemí, např. *CZ* pro Českou republiku; podle typu organizace použitím kódů, jako např. *com* pro komerční organizace; a podle funkce použitím kódů, jako např. *mil* pro servery americké armády.

Podobně jako domény nejvyšší úrovně, i domény DNS v rámci organizace mohou být mnoha způsoby strukturovány. Běžné domény, jako je například microsoft.com, jsou rovněž označovány jako nadřazené domény. Tímto názvem jsou označovány proto, že jsou nadřazené organizační struktuře. Nadřazené domény můžete rozdělit na poddomény, které můžete dále použít pro různé kanceláře, divize nebo umístění. Například plně kvalifikovaným názvem domény pro počítač v denverské pobočce firmy City Power & Light by mohl být workstation11.denver.cpandl.com. Kde *workstation11* je názvem počítače, *denver* je subdoménou a *cpandl.com* je nadřazenou doménou. Jiným výrazem pro subdoménu je *podřízená doména*.

Aktualizace služby DNS se provádí prostřednictvím jednoho autoritativního serveru DNS. Tento server je označen jako primární server DNS pro konkrétní doménu nebo oblast v doméně zvanou *zóna*. Primární server DNS obsahuje hlavní kopii záznamů DNS a konfigurační soubory domény. Sekundární servery DNS poskytují další služby usnadňující rozložení zátěže domény. Sekundární servery obsahují kopie záznamů DNS



Obrázek 1.3: Prostředí DNS se zónami

získané z primárního serveru při procesu zvaném *přenos zóny*. Sekundární servery získají své informace DNS od primárního serveru po svém spuštění a tyto informace si uloží, dokud nedojde k jejich aktualizaci nebo vypršení platnosti.

Na obrázku 1.3 je primární server DNS zodpovědný za domény DNS cpandl.com, data.cpandl.com a recs.cpandl.com. Sekundární servery DNS v doménách data.cpandl.com a recs.cpandl.com získají své informace DNS od tohoto primárního serveru při pravidelných přenosech zóny.

Služba Active Directory na službě DNS tak závisí, že buď byste měli službu DNS v síti nakonfigurovat před instalací služby Active Directory, nebo byste měli povolit Průvodci instalací služby Active Directory nainstalovat službu DNS za vás. Konfigurace služby DNS vyžaduje instalaci a konfiguraci klientů DNS a serverů DNS. Všechny operační systémy Windows obsahují klienty DNS a lze je nakonfigurovat pomocí plně kvalifikovaných názvů hostitelů. Každý počítač s operačním systémem Windows Server lze nakonfigurovat jako server DNS.

Pokud ve vaší síti nakonfigurujete službu Active Directory, můžete automaticky nainstalovat službu DNS jako součást instalace služby Active Directory. Rovněž můžete specifikovat, zdali mají být služby DNS a Active Directory částečně, nebo zcela integrovány. Jelikož integrace se službou Active Directory změní způsob fungování služby DNS, porozumění možnostem integrace je velmi důležité.

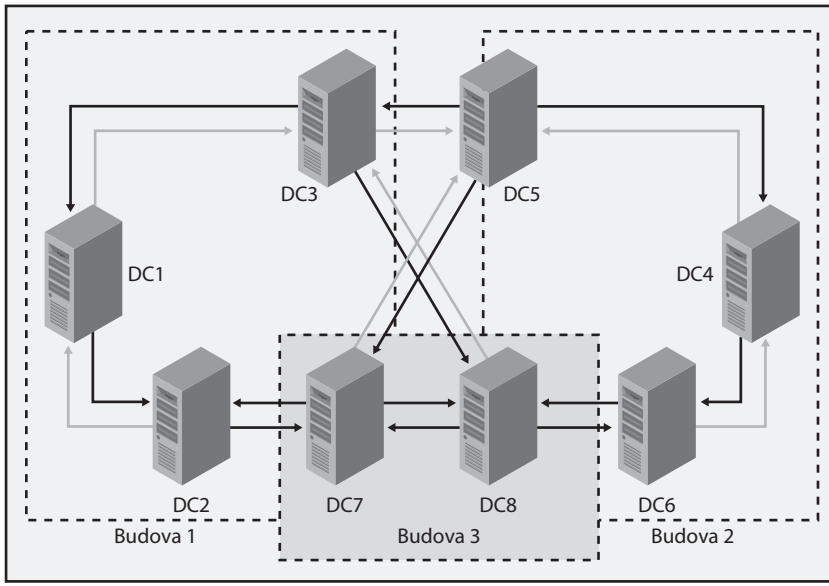
V případě částečné integrace doména použije standardní úložiště souborů a aktualizace služby DNS jsou zpracovány výše uvedeným způsobem. Doména obsahuje jeden primární server a jeden nebo více sekundárních serverů DNS. Sekundární servery DNS získají své informace DNS od primárního serveru DNS.

V případě úplné integrace jsou informace DNS uloženy přímo ve službě Active Directory. Jelikož tyto informace jsou součástí služby Active Directory, získáte všechny výhody služby Active Directory a vaše doména použije k aktualizaci a uchování informací DNS službu Active Directory.

Řadiče domény

Při instalaci systému Windows Server na určitý počítač můžete tento počítač nakonfigurovat jako samostatný server, členský server nebo řadič domény. *Řadič domény* (též DC) je počítač, na kterém je uložen adresář služby Active Directory. Pokud používáte systém Windows Server 2008, instalace služby Active Directory se bude skládat ze dvou kroků. Nejprve na server přidáte roli služby AD DS (Active Directory Domain Services) pomocí Průvodce přidáním rolí (Add Roles Wizard). Poté spusťte Průvodce instalací služby Active Directory. Pokud není služba DNS již nainstalována, budete k její instalaci vyzváni. Pokud neexistuje žádná doména, průvodce vám pomůže vytvořit doménu a nakonfigurovat v této nové doméně službu Active Directory. Průvodce vám může rovněž pomoci přidat podřízené domény k existujícím doménovým strukturám.

Podobně jako systémy Windows 2000 a Windows Server 2003, ani systém Windows Server 2008 neurčuje žádné primární nebo záložní řadiče domény. Místo toho systém Windows Server 2008 podporuje model replikace multimaster. V tomto modelu, který je znázorněn na obrázku 1.4, může změny adresáře zpracovat každý řadič domény a poté tyto změny automaticky replikuje na ostatní řadiče domény. Tím se tento model odlišuje od modelu replikace single-master, u kterého primární řadič domény obsahuje hlavní kopii, a záložní řadiče obsahují záložní kopie hlavního serveru. Navíc, systém Windows NT distribuoval pouze databázi SAM (Security Accounts Manager), ale systém Windows 2000 a novější verze systému Windows Server distribuují celý adresář informací týkající se distribuovaných prostředků.



Obrázek 1.4: Každý řadič domény může replikovat změny

Z praxe: Jelikož provádění některých změn pomocí replikace multimaster je nepraktické, služba Active Directory rovněž používá replikaci single-master. V takovém případě jeden nebo více řadičů domény, označených jako hlavní operační servery, provádí operace, které nelze provádět ve stejnou dobu na různých místech v síti.

Použití modelu multimaster službou Active Directory skýtá mnohé výhody týkající se výkonu a dostupnosti. Replikace multimaster vám umožní aktualizovat adresář v libovolném řadiči domény. Tento řadič domény postupně replikuje změny na ostatní řadiče domény. Pokud máte nasazeno více řadičů domény, replikace bude pokračovat, i když každý řadič domény selže.

Ačkoliv domény služby Active Directory mohou fungovat pouze s jedním řadičem domény, můžete a měli byste ve vašich doménách nakonfigurovat více řadičů domény. Pokud tak učiníte, tak v případě selhání jednoho řadiče domény se můžete spolehnout na jiný řadič domény, který zajistí autentizaci a převezme další důležité úlohy.

Řadiče domény řídí všechny aspekty uživatelské interakce s doménami služby Active Directory. Ověřují pokusy o přihlášení uživatelů, vyhledávají objekty a poskytují mnohé další služby. Ve službě Active Directory jsou informace o adresáři logicky rozděleny na oddíly. Každý řadič domény obsahuje kopii všech příslušných oddílů. Příslušné oddíly pro konkrétní řadič domény jsou určeny umístěním řadiče domény a způsobem, jakým je řadič domény použit.

Řadiče domény zajišťují změny informací, které uchovávají, a odpovídajícím způsobem replikují tyto změny na ostatní řadiče domény. Kvůli způsobu, jakým replikace funguje, může nastat konflikt, jestliže se na určitém řadiči domény změní některý atribut, protože na jiném řadiči domény je rozšířena změna téhož atributu. Služba Active Directory rozpozná konflikt porovnáním čísla verze vlastnosti každého atributu (což je hodnota, která se inicializuje při vytvoření atributu a aktualizuje se při každé jeho změně) a replikací změněného atributu s vyšším číslem verze vlastnosti.

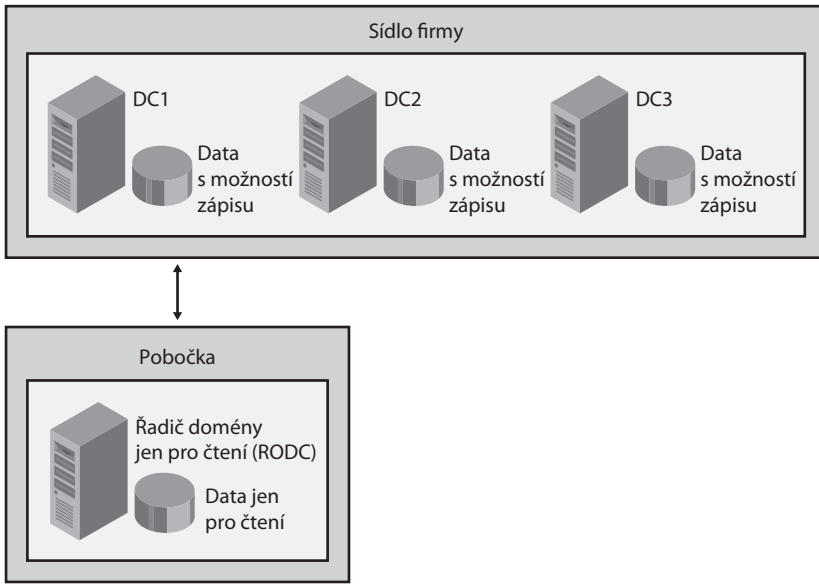
Běžně jsou řadiče domény určeny pro čtení a pro zápis. Ovšem systém Windows Server 2008 a novější verze podporují také řadiče domény jen pro čtení. *Řadič domény jen pro čtení* (RODC) je řadičem domény, který je hostitelem repliky adresáře domény, jež je určena jen pro čtení. Standardně nejsou na řadičích domény jen pro čtení uložena žádná hesla nebo pověření kromě těch, která se používají jen pro jejich vlastní účet počítače a účet Kerberos Target (krbtgt). Díky tomu jsou řadiče domény jen pro čtení ideální pro pobočky, v nichž nelze zaručit fyzické zabezpečení řadiče domény.

Obrázek 1.5 znázorňuje řadič domény jen pro čtení nasazený na pobočce. Sídlo firmy obsahuje více řadičů domény s daty pro zápis. Pobočka obsahuje řadič domény jen pro čtení s daty jen pro čtení. Řadič domény jen pro čtení je umístěn na pobočce, neboť nelze zaručit fyzické zabezpečení serveru.

Tip: Kromě hesel uchovává řadič domény jen pro čtení stejné objekty a atributy jako řadiče domén s možností zápisu. Tyto objekty a atributy jsou replikovány na řadiče domény jen pro čtení pomocí jednosměrné replikace z řadiče domény s možností zápisu, který slouží jako partnerský server pro replikaci. Ačkoliv řadiče domény jen pro čtení mohou získat informace od řadičů domény se systémem Windows Server 2003, aktualizace oddílu domény mohou řadiče domény jen pro čtení získat pouze od řadiče domény s možností zápisu se systémem Windows Server 2008, který se navíc nachází ve stejné doméně.

Řadiče domény jen pro čtení si vyžádají pověření uživatele a počítače od řadiče domény s možností zápisu se systémem Windows Server 2008. Potom, je-li to povoleno Zásadami replikací hesel, které jsou vynuceny na řadiči domény s možností zápisu, řadiče

domény jen pro čtení podle potřeby uloží pověření do mezipaměti, dokud se pověření nezmění. Jelikož na řadičích domény jen pro čtení jsou uloženy pouze podmnožiny pověření, pověření, která by mohla být eventuálně kompromitována, jsou omezena.



Obrázek 1.5: Řadič domény jen pro čtení nasazený na pobočce

Objekty služby Active Directory

Prostředky, které chcete reprezentovat ve službě Active Directory, jsou vytvořeny a uloženy jako objekty. Objekty mají atributy, které definují druh informací, jež chcete o těchto prostředcích uložit. Například objekt Uživatel (User) v Active Directory obsahuje atributy, které pomáhají popsat uživatele, tedy např. jméno, iniciálu druhého jména, příjmení a zobrazované jméno. Objekt Počítač (Computer) v Active Directory obsahuje atributy, které pomáhají popsat počítače, tedy např. název počítače, popis, umístění a identifikátor zabezpečení.

Objekty v adresáři jsou buď koncové objekty stromové struktury, nebo kontejnery. Objekty, které nemohou obsahovat jiné objekty, jsou *koncové objekty stromové struktury*, nebo zjednodušeně řečeno *listy*. Objekty, které obsahují jiné objekty, se označují jako *objekty kontejneru*, nebo zjednodušeně řečeno *kontejnery*. Samotný adresář je kontejnerem, který obsahuje jiné kontejnery a objekty. Na obrázku 1.6 je objekt Users kontejnerem, který obsahuje objekty třídy Uživatel (User), objekt Computers je kontejnerem, jenž obsahuje objekty třídy Počítač (Computer), a objekt Printers je kontejnerem, který obsahuje objekty třídy Tiskárna (Printer).