KAPITOLA

7

# Instalujeme doménu

**Témata kapitoly:**

- Co je to Active Directory?
- Co když doména nestačí?
- Na jaké místo doménu logicky zařadit?
- Co musí být před instalací domény připraveno?
- Instalace domény Active Directory
- Konfigurace přihlášení k počítači
- Závěr

V kapitole 5, „Jak růst s firmou?“, jsme provedli krátké porovnání prostředí pracovní skupiny a domény. Zároveň jsme uvedli, že prostředí domény je rozumné pro střední a velké sítě, ve kterých by správa uživatelských účtů v pracovní skupině již byla nikdy nekončící a vyčerpávající dřina.

Kromě jednodušší správy účtů nabízí doména ještě další a další funkce týkající se správy ostatních objektů, které se v síti běžně vyskytují. Umožňuje provádět jednoduchou a automatickou instalaci operačního systému dalších klientských počítačů, jejich aplikací, určovat úroveň zabezpečení počítačů a například i určit, jak který klientský počítač bude pracovat a co bude či nebude konkrétní uživatel smět provádět. To vše lze provádět z jediného místa a samozřejmě pouze s patřičnými znalostmi.

Co to vlastně doména je, jak vypadá v prostředí systému Windows Server 2003 a jak se instaluje, si uvedeme v dalších částech této kapitoly.

## Co je to Active Directory?

Doména je vlastně databází, která by měla obsahovat všechny objekty v síti (správná doména tyto objekty obsahuje). To znamená, že v doméně by se měly objevit například veškeré účty uživatelů, skupiny uživatelů, účty počítačů, informace o tiskárnách a informace o dalších objektech. Tyto další objekty sice nebývají pro správce tak „viditelné“, jako jsou například uživatelské účty, ale jsou reprezentací některých prvků sítě, a měly by tedy rozhodně součástí domény být.

Domény tedy lze představit jako logické seskupení objektů v síti. U drtivé většiny objektů totiž vůbec není podstatné, na jakém fyzickém místě v síti se nacházejí, některé objekty takový atribut ani nemají.

Doména neboli doménová databáze však není jen seskupení objektů. Této databáze se také lze dotazovat na různé věci (například v jakém oddělení pracuje uživatel Jaro-

slav Hluboký). A protože databáze na položené dotazy odpovídá (a odpovídá na ně dobře), plní roli i jakési služby (služby doménové databáze jsou mnohem rozsáhlejší, pro tuto kapitolu to však není podstatné). Doménu tedy můžeme nazvat databázovou službou a pokud si za slovo „databázovou" dosadíte častěji používané slovo „adresářovou", dostáváte označení „adresářová služba". A **názvem** adresářové služby se systémem Windows Server 2003 (stejně jako Windows 2000 Server) je **Active Directory**.

Active Directory (AD) je tedy hierarchické úložiště, které zároveň nabízí snadný přístup k uloženým informacím o veškerých prostředcích v síti. Pomáhá uživatelům a aplikacím tyto prostředky nalézt a přistupovat k nim, navíc zajišťuje, že se k informacím dostane pouze oprávněná osoba, tedy taková, která má potřebné oprávnění. I tato oprávnění jsou uložena v databázi Active Directory.

## Řadič domény

Počítač, který plní roli serveru s adresářovou službou, se nazývá *řadič domény*. Jinými slovy – řadič domény je počítačem, ve kterém je uložena celá databáze Active Directory. Všechny dotazy na adresářovou službu nebo obecně všechny požadavky na přístup k informacím uloženým v doméně vyřizuje právě takový počítač.

Role řadiče domény je tak v síti velmi důležitou rolí, na které velmi výrazně závisí správná funkce sítě. Proto se i k počítačům plnícím roli řadiče domény (DC, Domain Controller) přistupuje opatrněji než k ostatním počítačům. Proto mívají tyto počítače vyšší stupeň zabezpečení (jak z pohledu domény, tak i fyzického), instalují se na spolehlivý a dostatečně vybavený hardware. Navíc se málokdy (to platí zejména pro větší prostředí) využívají jako servery plnící další role, například aplikační, databázové, souborové či tiskové servery.

Každá společnost s doménovým modelem začne vždy instalací prvního řadiče domény. Žádný řadič domény však není vždy stoprocentní, a může se stát, že za nějaký čas používání odejde jeho hardwarová (například paměť nebo pevný disk) nebo jiná důležitá součást. Co se v takovém případě může stát?

Protože je řadič domény jediným počítačem, který udržuje databázi Active Directory, nebude v případě jeho výpadku tato databáze k dispozici. Znamená to, že uživatelé se nebudou moci přihlašovat pomocí svých doménových účtů, nebudou moci získat přístup k prostředkům v síti a podobně. Protože se však výpadku řadiče domény předejít nedá, je nutné tuto situaci vyřešit již při plánování domény. Řešením je v takovém případě více řadičů domény.

### Více řadičů domény

Každému uživateli stačí k práci v prostředí domény jediný uživatelský účet. Pokud je však v doméně více řadičů domény, nebude to s jediným uživatelským účtem v rozporu? Nebude! Při instalaci dalšího řadiče domény nedochází k vytvoření nové databáze Active Directory, ale vytvoří se takzvaná *replika* stávající. Každý řadič domény tak bude udržovat stejné adresářové informace (včetně uživatelských účtů).

Pokud v takovémto prostředí přestane jeden z řadičů domény pracovat, začnou se klienti automaticky obracet na jiný, a jejich práce tak nebude přerušena ani ztížena.

# Co když doména nestačí?

Otázku Co když doména nestačí? nelze chápat tak, že existuje ještě lepší model správy prostředí sítě než je doménový. Je třeba se na ni podívat z pohledu síťového prostředí, které nelze do jedné domény vměstnat (možná by tedy bylo lepší napsat „Co když jedna doména nestačí?“). Nejde o to, že by doména Active Directory byla omezena počtem objektů. Ona tedy je omezena počtem několika milionů objektů, ale to nás jistě trápit nemusí. Je to však výrazný pokrok oproti doméně se systémem Windows NT 4.0, která byla omezena počtem 40 tisíc objektů (i když i toto omezení bylo v našich zeměpisných šířkách nedosažitelné).

V praxi se skutečně může někdy stát, že jediná doména nebude pro správu celého prostředí postačovat. Uveďme si situace, kdy k takovému stavu může dojít.

- **Politické rozhodnutí** Tedy rozhodnutí vedení společnosti. Správci sice tato rozhodnutí nijak nevítají, nicméně ve většině případů je musí respektovat.
- **Jedinečné zásady** Pokud bude mít organizace například požadavek, že hesla uživatelů z oddělení vývoje musí být dlouhá nejméně 10 znaků, zatímco hesla ostatních uživatelů musí být dlouhá „pouhých“ 8 znaků, je to důvod pro vytvoření další domény. Dva či více různých požadavků na tuto zásadu nelze v prostředí jediné domény aplikovat.
- **Vytížení síťových linek** Když se v doméně vytvoří nový uživatelský účet (nebo jiný objekt), dochází k jeho replikaci na všechny řadiče domény. Pokud bude mít organizace například dvě pobočky, které budou spojeny nespolehlivou a pomalou linkou, nebude možná chtít, aby byla tato linka zatěžována replikacemi adresářové služby. Řešení takového požadavku je ve vytvoření další domény.
- **Požadavky na názvy domén** Název stávající domény nemusí organizaci vyhovovat například pro uživatele z nového oddělení nebo nové pobočky. Vzhledem k tomu, že doména nemůže mít více názvů, je řešením instalace další domény.

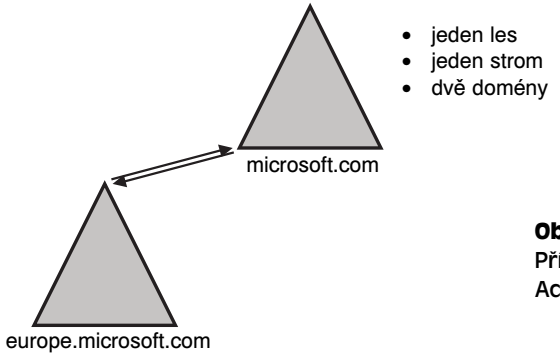
V praxi se v našich zeměpisných šířkách lze setkat s prostředími, která mají více domén. Jedná se však spíše o pobočky zahraničních společností nebo o velmi velká prostředí. Pokud se vaší organizace nebude týkat žádná z výše uvedených poznámek, jistě vystačíte s jedinou doménou.

## Stromy Active Directory

Pokud má jedna organizace více domén, má dvě možnosti, jak je logicky uspořádat. První z možností je takzvaný doménový strom.

Doménový strom se vyznačuje tím, že všechny jeho domény sdílejí souvislý obor názvů. Znamená to, že název domény v nejvyšší úrovni (tzv. *kořenové domény*) se vyskytuje na konci názvu každé podřízené domény. V uvedeném příkladu se název podřízené domény skládá ze slova *europe* a z názvu kořenové domény (*microsoft.com*).

Mezi všemi doménami stromu Active Directory (a jejich počet není omezen) existují takzvané vztahy důvěryhodnosti. V praxi to znamená, že například uživatelé, kteří mají své účty v doméně *microsoft.com*, mohou získat prostřednictvím svého doménového účtu přístup ke sdílené složce v doméně *europe.microsoft.com*, samozřejmě za předpokladu, že jim jej správce domény *europe.microsoft.com* udělí. Tyto vztahy důvěryhodnosti se vy-




**Obrázek 7.1**
**Příklad stromu Active Directory**

tvářejí automaticky během instalace nových domén a nesou si s sebou dvě významné vlastnosti:

- **Vztahy důvěryhodnosti jsou obousměrné** V uvedeném příkladu to znamená, že uživatelé z domény *microsoft.com* mohou přistupovat k prostředkům v doméně *europe.microsoft.com* a naopak, uživatelé z domény *europe.microsoft.com* mohou přistupovat k prostředkům v doméně *microsoft.com*.
- **Vztahy důvěryhodnosti jsou přenosné (tranzitivní)** Pokud si mezi sebou navzájem důvěřují domény *microsoft.com* a *europe.microsoft.com* a *microsoft.com* a *asia.microsoft.com*, znamená to, že si automaticky důvěřují také domény *europe.microsoft.com* a *asia.microsoft.com*. Není tedy nutné vytvářet mezi posledními dvěma jmenovanými doménami ručně vztah důvěryhodnosti.

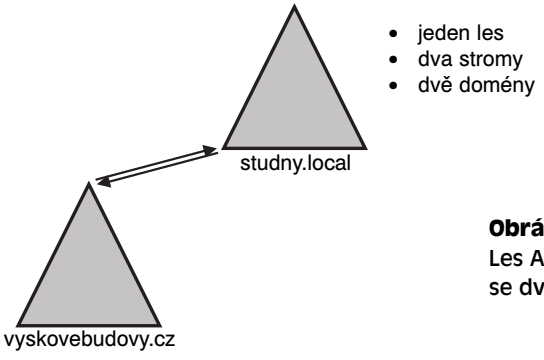
## Lesy Active Directory

Organizace, která má jednu doménu (tedy jeden strom) nebo více domén (stále jeden strom), může například koupit jinou zavedenou společnost. Například řekněme, že organizace Studny, s.r.o. koupí společnost Výškové budovy, a.s.

Organizace Studny, s.r.o. může mít svou doménu Active Directory s názvem *studny.local* a společnost Výškové budovy, a.s. může mít také svou doménu s názvem *vyskovebudovy.cz*. Cílem spojení společností bude jistě mimo jiné propojit i svou síťovou infrastrukturu a správu domén. Řešením takové situace je spojit dvě domény do jedné struktury, požadavek však může znít tak, že obě domény si musí ponechat své názvy (důvodem takového rozhodnutí mohou být například požadavky používaných aplikací nebo zvyklosti uživatelů).

Vzhledem k naprosto odlišným (tedy nesouvislým) názvům již nelze zvažovat jako výslednou strukturu jediný strom Active Directory, ale stromy dva. Protože je však nutné tyto domény z pohledu jejich správy spojit, je řešením vytvořit dva stromy, oba v jediném lese Active Directory.

I mezi dvěma doménami z různých stromů v rámci stejného lesa existují automaticky obousměrné a přenosné vztahy důvěryhodnosti. Proto lze toto prostředí spravovat mnohem efektivněji než kdyby domény zůstaly naprosto oddělené.




**Obrázek 7.2**
Les Active Directory se dvěma stromy

Nyní jsme se přenesli do poněkud jiných prostředí, než které je naším cílem v této knize pochopit a naučit se spravovat, pro hrubou představu o možných strukturách Active Directory je ale dobré mít o těchto modelech alespoň základní informace. Zde totiž možnosti logických struktur Active Directory končí. Nutno dodat, že stejně jako počet domén ve stromu není omezen ani počet stromů v lese.

Dovedete si nyní představit prostředí se dvěma lesy Active Directory? Pokud ano, je vše v pořádku, pokud ne, zde je řešení: představte si například strukturu Active Directory společnosti Microsoft (uvedenou jako příklad na obrázku 7.1) a k tomu doménu Active Directory své společnosti. Ano, pokud se mluví o více lesech, jedná se o naprosto nezávislá prostředí, a ve většině případů tedy o naprosto nezávislé společnosti.

Otázka na závěr: Pokud nainstalujete jedinou doménu Active Directory, kolik existuje stromů a kolik lesů Active Directory?

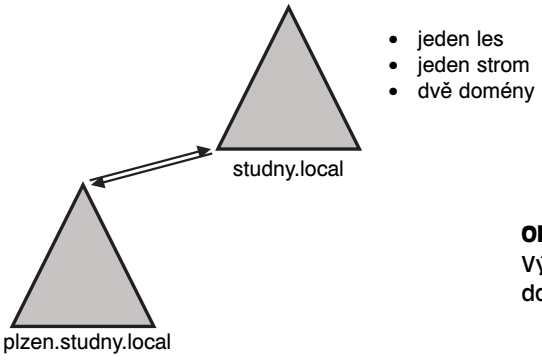
# Na jaké místo doménu logicky zařadit?

Odpověď na tuto otázku je tím jednodušší, čím menší prostředí budeme instalovat. Vzhledem k tomu, že každé prostředí má jedinou kořenovou doménu Active Directory (to je doména, která byla nainstalovaná jako první), je v případě instalace jediné domény situace naprosto jednoznačná. Zajímavější to začíná být v případě, kdy má mít společnost více domén. Pojďme se podívat na několik případů.

### Prostředí s více doménami, pokud již doména Active Directory existuje

Příkladem takové situace může být společnost se sídlem v Praze s již nainstalovanou doménou Active Directory. Kořenová doména tedy již existuje, a pokud musí dojít k instalaci další domény (například pro pobočku v Plzni), musí to být buďto podřízená doména té stávající (výsledkem bude jediný strom) nebo první doména nového stromu. Zde je však nutné připomenout, že důvodem pro vytvoření dalšího stromu je čistě jen udržení původního názvu, což je u nově instalované domény bezpředmětné.

Výsledná struktura domén Active Directory by mohla být podobná té na obrázku 7.3.

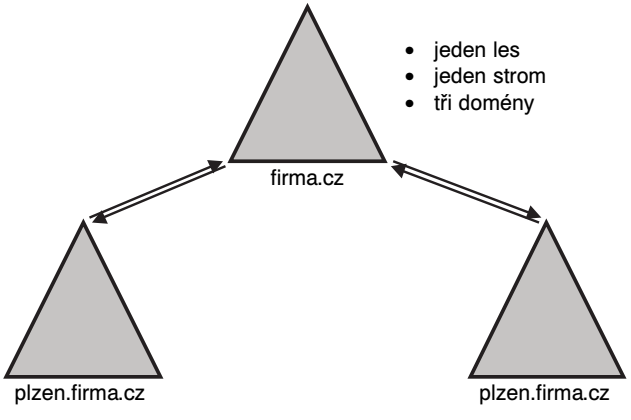



**Obrázek 7.3**
**Výsledná struktura domén Active Directory**

### Prostředí s více doménami, pokud žádná doména neexistuje

Příkladem této situace může být podobná firma, která se chystá nainstalovat prostředí Active Directory a již v tuto chvíli ví, že bude potřebovat více domén. Výsledný model může být stejný jako v předchozím případě, může však také vypadat úplně jinak. Z hlediska správy je mnohem přehlednější vědět, že uživatelé v sídle společnosti v Praze budou členy domény s názvem *praha.firma.cz* a uživatelé v pobočce Plzeň budou členy domény *plzen.firma.cz*. Další rozšiřování firmy by tak bylo z pohledu správy prostředí konzistentní a všechny domény by byly na stejné úrovni.

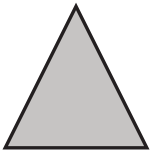
Jak ale v takovém případě celý model vyřešit? Vždyť dříve bylo uvedeno, že vždy musí existovat pouze jediná kořenová doména, od které se odvíjejí názvy podřízených domén. Jak to může dopadnout, ukazuje obrázek 7.4.




**Obrázek 7.4**
**Výsledná struktura domén Active Directory**

### Prostředí s jedinou doménou

V tomto případě není z pohledu návrhu doménového modelu co řešit. Výsledné prostředí bude sestávat z jediného lesa o jednom stromu obsahujícím jedinou doménu Active Directory. Mimochodem, všimli jste si, že zde je uvedena odpověď na otázku z odstavce Lesy Active Directory?




**Obrázek 7.5**
Výsledná struktura Active Directory

## Jaký má mít doména název?

Názvy domén Active Directory se v porovnání s doménami se systémem Windows NT 4.0 změnily. Nyní odpovídají názvům, na které jsme zvyklí z Internetu. Zatímco například dříve by se doména jmenovala *FIRMA*, nyní má navíc ještě příponu (například *FIRMA.CZ*).

Samostatný název FIRMA je názvem rozhraní NetBIOS, zatímco název FIRMA.CZ je názvem DNS. Názvy NetBIOS využívají systémy starší než Windows 2000, názvy DNS využívají primárně systémy Windows 2000, Windows XP a řada systémů Windows Server 2003. Z důvodu zpětné kompatibility je tedy nutné definovat stále názvy oba a doména Active Directory tak i nadále vystupuje. Pro klientské počítače se systémem Windows NT 4.0 Workstation tak bude vystupovat pod názvem FIRMA, zatímco pro klienty se systémem Windows XP Professional pod názvem FIRMA.CZ.

Pokud se rozhodnete nainstalovat doménu Active Directory se systémem Windows 2000 Server, je nutné velmi pečlivě zvolit její název, neboť ten později není možné změnit. Název kořenové domény určuje „elektronickou identitu" společnosti. Od něj se odvíjejí názvy případných dalších domén ve stejném stromu. Při jeho volbě je nutné dbát na požadavky vedení společnosti, na znalosti uživatelů, na existenci či neexistenci názvu domény v Internetu a na způsob vedení záznamů zóny DNS internetové domény.

## Volba přípony názvu domény

Nedílnou součástí názvu domény je její přípona. Při plánování nasazení domény Active Directory stojí většina firem před rozhodnutím, zda použít:

- **Příponu, kterou lze použít v Internetu** Pokud má například společnost prezentaci v Internetu pod názvem *firma.cz*, může tuto příponu použít i v názvu domény Active Directory. Pokud společnost prezentaci nemá, může tento název samozřejmě použít také a v Internetu se prezentovat později.
- **Příponu, kterou nelze v Internetu použít** Bez ohledu na internetovou prezentaci může společnost použít v názvu domény Active Directory příponu, která se v Internetu nemůže objevit (například *local*).

Každá volba má své výhody i nevýhody a záleží na konkrétním případu, co bude pro společnost výhodnější. Obecně platí, pokud společnost má nebo plánuje prezentaci v Internetu (například *firma.cz*), měl by být název interní domény Active Directory jiný a takový, který se v Internetu nemůže objevit (například *firma.local*). Takové řešení je pro správce přehlednější, pokud si navíc společnost sama vede zónu DNS pro svou internetovou prezentaci, je možné správu této zóny oddělit od správy zóny DNS pro potřeby domény Active Directory.

Protože naše společnost Studny, s.r.o. jistě bude mít v budoucnu vlastní internetovou prezentaci, zvolíme název domény podle výše uvedeného doporučení na ***studny.local***.

Pokud budete instalovat doménu se systémem Windows 2000 Server, je třeba věnovat jejímu názvu pečlivou pozornost, neboť později nelze rozhodnutí změnit. Doména Active Directory se systémy Windows Server 2003 umožňuje změnu názvu, pouze však za použití speciálního nástroje Domain Rename Tool, který je k dispozici na instalačním disku CD-ROM se systémem Windows Server 2003 nebo jejž lze stáhnout z webových stránek společnosti Microsoft.

# Co musí být před instalací domény připraveno?

Stejně jako na jakoukoli jinou instalaci je nutné se připravit také na instalaci domény Active Directory. Dále je uveden seznam všech náležitostí, které je vhodné (a ve většině případů nezbytné) dopředu připravit. Vše se týká instalace kořenové domény Active Directory, která bude později provedena.

- **Operační systém** Roli řadiče domény lze nainstalovat pouze v serverovém operačním systému. Budeme tedy potřebovat některý ze systémů řady Windows Server 2003.
- **Potřebná oprávnění** V případě instalace prvního řadiče kořenové domény je nutné přihlásit se jako místní správce počítače.
- **Název DNS domény** Pro naši doménu jsme určili název DNS *studny.local*. Další informace k názvům domén jsou uvedené výše.
- **Název NetBIOS domény** Tento název je určený pro klientské operační systémy nižší než Windows 2000, které primárně využívají názvy NetBIOS. Instalační program standardně nabízí jako název NetBIOS první část názvu DNS (v našem případě *studny*). Ve většině případů jej můžete ponechat.
- **Umístění důležitých souborů domény** Během instalace je nutné určit umístění databáze Active Directory a protokolů transakcí a složky SYSVOL. Databázi a protokoly transakcí lze kdykoli později přesunout na jiné místo, složky SYSVOL nikoli.
- **Kompatibilita oprávnění s nižšími systémy** Pokud budou v síti pouze servery se systémy řady Windows Server 2003 nebo Windows 2000 Server, není nutné zachovávat oprávnění kompatibilní s nižšími systémy. Toto nastavení se netýká operačních systémů klientských počítačů.
- **Heslo pro obnovení adresářové služby** Pokud byste v budoucnu potřebovali provést obnovení domény Active Directory ze zálohy, je nutné řadič domény spustit v režimu obnovení adresářové služby a přihlásit se pomocí účtu Administrator a hesla zadaného v tomto kroku instalace domény.

**Poznámka**

**Toto heslo je jedno z nejdůležitějších. Není nic horšího, než po dvou letech, kdy se náhle vyskytne nutnost obnovit doménu Active Directory, zjistit, že toto heslo neznáte. V takovém případě samozřejmě máte smůlu (kterou jste si ale zavinili sami) a doménu Active Directory neobnovíte.**

- **Síťové součásti** Server, který se stane řadičem domény, musí mít správně nakonfigurované síťové součásti a jeho síťové připojení musí být aktivní (síťový adaptér musí být připojen k síti).

## Služba DNS

Adresářová služba Active Directory je úzce spjata se službou DNS. Tak úzce, že se bez ní neobejde. Využívá ji k vyhledávání informací v síti, stejně tak ji využívají klientské počítače při vyhledávání důležitých služeb v síti. Služba DNS je tedy dalším nutným předpokladem pro správnou funkci domény Active Directory.

V naší síti jsme službu DNS nainstalovali již dříve a vytvořili jsme zónu DNS s názvem odpovídajícím zamýšlenému názvu domény Active Directory *studny.local*. Vzhledem k tomu, že služba DNS je skutečně nedílnou součástí domény Active Directory, nabízí v případě její nepřítomnosti průvodce instalací domény její automatickou instalaci a konfiguraci.

Tohoto průvodce a tento postup lze doporučit v případech, kdy počítač, do kterého se právě instaluje role řadiče domény, bude zároveň serverem DNS. Pokud je v síti více počítačů a řadič domény nebude stejný se serverem DNS, je nutné nainstalovat a nakonfigurovat službu DNS před instalací domény.

# Instalace domény Active Directory

V další části provedeme instalaci domény Active Directory do počítače SRVR001. Poté provedeme kontrolu instalace a do domény vložíme všechny klientské počítače (PC001…). Na závěr provedeme několik konfiguračních úkonů důležitých pro zabezpečení domény a zejména zóny DNS.

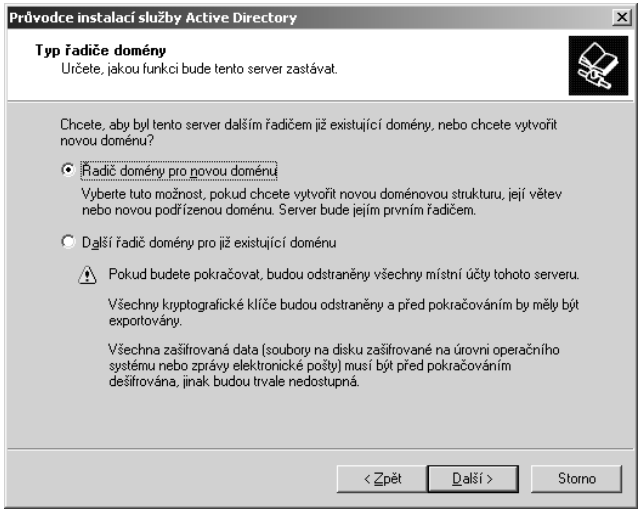
## Instalace domény

1. Přihlaste se k serveru **SRVR001** jako správci. V nabídce **Spustit** zadejte příkaz `cmd` a poté na příkazovém řádku zadejte příkaz `dcpromo`. Spustí se **Průvodce instalací služby Active Directory**. Klepněte na tlačítko **Další**.
2. V dialogovém okně **Kompatibilita s operačními systémy** si přečtěte uvedené informace a poté klepněte na tlačítko **Další**.

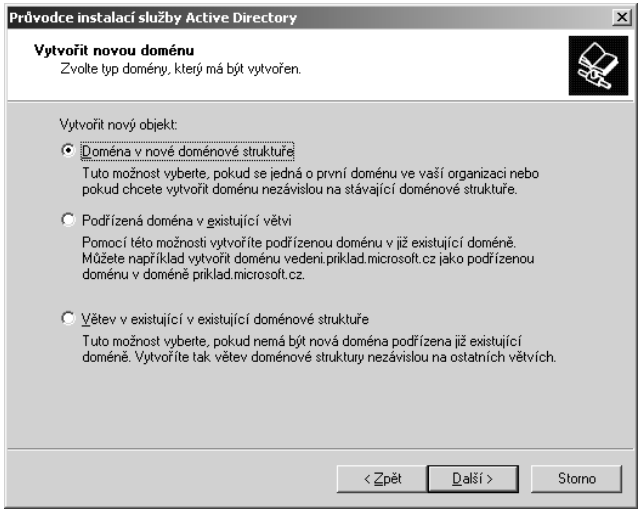
   **Poznámka**

   **Uvedené informace se týkají operačních systémů Windows 95 a Windows NT 4.0 s aktualizací SP3 nebo nižší. Protože tyto operační systémy v síti nebudou, nemusejí nás tyto informace zajímat. Pokud by v síti tyto systémy byly, není v tuto chvíli možné dělat nic jiného, než pokračovat klepnutím na tlačítko Další.**

3. V dialogovém okně **Typ řadiče domény** ponechte zaškrtnuté políčko **Řadič domény pro novou doménu** a poté klepněte na tlačítko **Další**.
4. V dialogovém okně **Vytvořit novou doménu** ponechte zaškrtnuté políčko **Doména v nové doménové struktuře** a poté klepněte na tlačítko **Další**.




**Obrázek 7.6**
Vytvoření nové domény Active Directory




**Obrázek 7.7**
Vytvoření nového lesa Active Directory

**Poznámka**

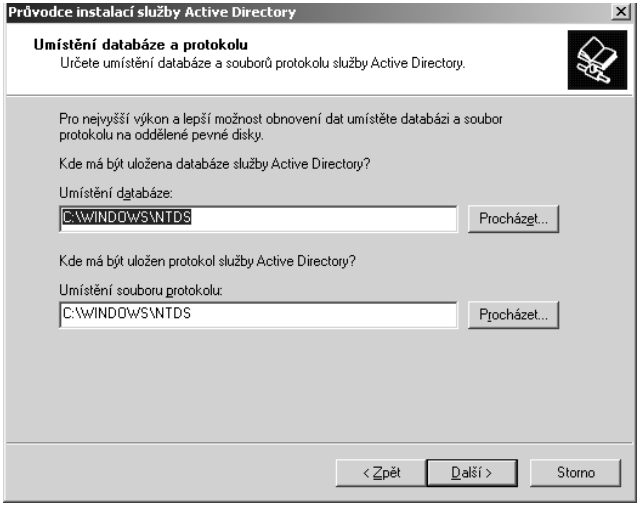
**Pojem Podřízená doména v existující větvi odpovídá instalaci podřízené domény do stávajícího stromu. Pojem Větev v existující doménové struktuře odpovídá vytvoření nového stromu.**

5. V dialogovém okně **Název nové domény** zadejte do pole **Úplný název DNS nové domény** řetězec **studny.local** a poté klepněte na tlačítko **Další**.
6. V dialogovém okně **Název domény v systému NetBIOS** ponechte v poli **Název domény pro rozhraní NetBIOS** název **STUDNY** a pokračujte klepnutím na tlačítko **Další**.

7. V dialogovém okně **Umístění databáze a protokolu** ponechte výchozí cesty **C:\WINDOWS\NTDS** pro databázi a **C:\WINDOWS\NTDS** pro soubory protokolů transakcí. Poté klepněte na tlačítko **Další**.

**Poznámka**

Z hlediska optimalizace a výkonu řadiče domény je optimální umístit soubory protokolů transakcí na jiný **fyzický** disk, než na kterém je umístěna databáze Active Directory. V našem případě nemáme jiný disk k dispozici, takže ponecháme navržené umístění.



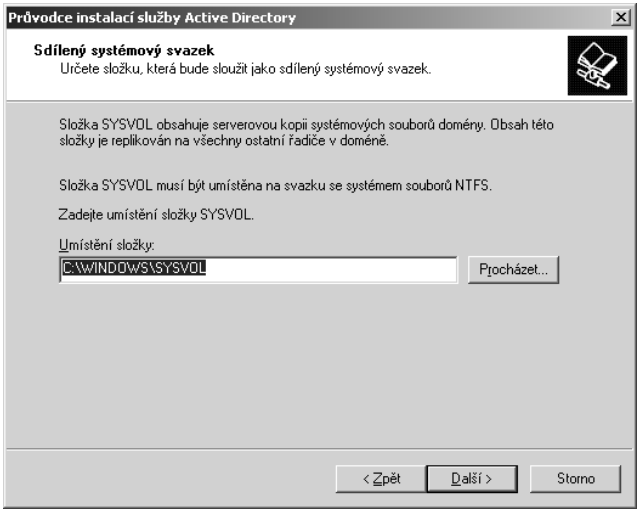

**Obrázek 7.8**
Uložení databáze domény Active Directory a protokolů transakcí

8. V dialogovém okně **Sdílený systémový svazek** ponechte výchozí cestu **C:\WINDOWS\SYSVOL** a poté klepněte na tlačítko **Další**.

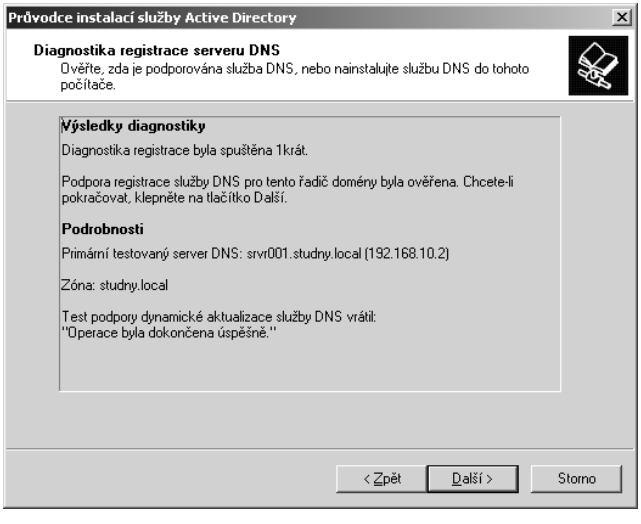
**Poznámka**

Svazek SYSVOL není možné později přesunout. Zde je nutné zajistit, aby byl v jednotce, která má dostatek volného místa. Jak uvidíme později, bude obsahovat objekty zásad skupiny, které jeho velikost zvětšují, a pokud by na disku nebyl dostatek místa, můžete mít s funkčností domény problémy.

9. Nyní server provede vyhledání zóny DNS s názvem odpovídajícím zadanému názvu domény. Pokud zónu nalezne, zobrazí informaci o úspěšně provedené diagnostice. Pokud zónu nenalezne, nabídne její automatickou instalaci a konfiguraci. Po přečtení informací klepněte na tlačítko **Další**.
10. V dialogovém okně **Oprávnění** ponechte zaškrtnuté políčko **Oprávnění kompatibilní pouze s operačními systémy řady Windows 2000 Server nebo Windows Server 2003** a poté klepněte na tlačítko **Další**.
11. V dialogovém okně **Heslo správce režimu obnovení adresářových služeb** zadejte do pole **Heslo pro režim obnovení** a do pole **Potvrzení hesla** heslo, které použijete při případném obnovení databáze Active Directory ze zálohy. Poté klepněte na tlačítko **Další**.




**Obrázek 7.9**
Uložení sdílené replikované složky SYSVOL




**Obrázek 7.10**
Výsledky pokusu o vyhledání zóny DNS studny.local

### Poznámka

Nepoužívejte stejné heslo, jako je heslo běžného účtu správce. Heslo správce domény by se totiž mělo pravidelně měnit, zatímco toto heslo zůstává stejné. V praxi by se poté mohlo stát, že například po dvou letech činnosti bude nutné obnovit doménu Active Directory a na heslo pro tento režim si nevzpomenete. Proto je dobré zadané heslo ihned po zadání zaznamenat a uložit na bezpečné místo.

Pokud byste v budoucnu instalovali další řadič domény, nemusí být toto heslo stejné. Znovu je dobré si heslo zaznamenat, samozřejmě i s názvem počítače, ke kterému se váže.

12. V dialogovém okně **Souhrn** prověřte správnost konfigurace všech parametrů domény Active Directory. V případě nepřesností se opakovaným klepnutím na tlačít-

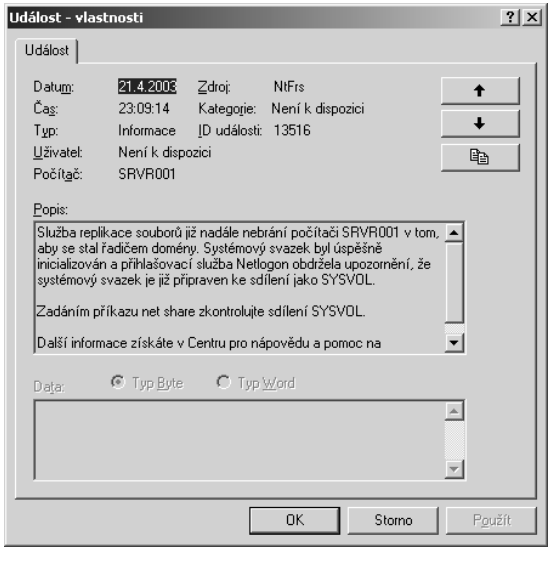
ko **Zpět** vraťte k danému dialogovému oknu a hodnotu opravte. Pokud souhlasíte, klepněte na tlačítko **Další**. Tím se spustí instalace řadiče domény.

13. Po dokončení Průvodce instalací služby Active Directory je nutné počítač restartovat.

## Ověření správné instalace řadiče domény

Server SRVR001 je nyní řadičem domény Active Directory *studny.local*. Po instalaci každého řadiče domény je vhodné provést kontrolu správné instalace:

1. K počítači **SRVR001** se přihlaste jako správci. Účet **Administrator** je nyní jediný účet s nejvyššími oprávněními v doméně **studny.local**.
2. Spusťte aplikaci **Průzkumník Windows** a ověřte, zda existuje složka **C:\WINDOWS\NTDS** se soubory **NTDS.DIT** (databáze Active Directory) a **EDB.LOG** (soubor protokolů transakcí). Dále ověřte existenci složky **C:\WINDOWS\SYSVOL**.
3. V **Nabídce Start** přejděte na položku **Nástroje pro správu** a ověřte, zda mezi nástroji přibyly nástroje týkající se správy domény – například nástroje **Uživatelé a počítače služby Active Directory**, **Sítě a služby Active Directory** či **Zásady zabezpečení domény**. Poté klepněte na nástroj **Prohlížeč událostí** a ověřte, že zde přibyly položky **Adresářová služba** a **Služba replikace souborů**. Klepněte na položku **Služba replikace souborů** a vyhledejte událost **13516**. Ta oznamuje, že řadič domény plní svoje funkce.




**Obrázek 7.11**
Událost 13516 v protokolu Služby replikace souborů

4. Spusťte konzolu **DNS** a ověřte, že v zóně **studny.local** došlo k vytvoření poddomén **_msdcs**, **_sites**, **_tcp**, **_udp**, **DomainDnsZones** a **ForestDnsZones**. První čtyři poddomény jsou z hlediska funkčnosti domény Active Directory velmi důležité. Obsahují totiž takzvané záznamy **SRV** (Umístění služby – Service location), podle kterých se orientují všechny počítače se systémy Windows 2000/XP/2003 v síti při hledání důležitých služeb.

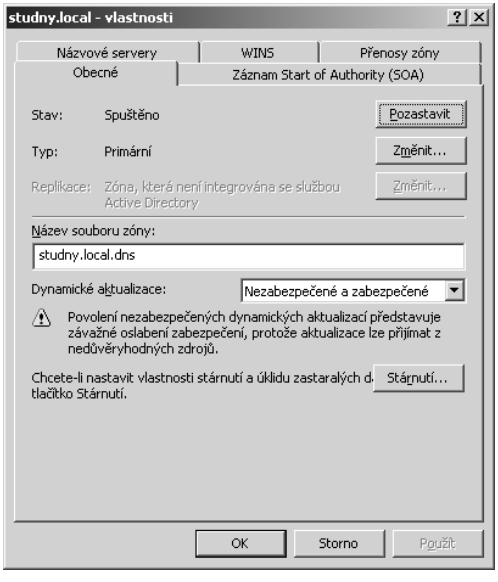
5. Na příkazovém řádku zadejte příkaz `net share`. Zobrazí se sdílené složky počítače včetně položky **NETLOGON** směrované do složky **C:\WINDOWS\SYSVOL\studny.local\SCRIPTS**.

**Poznámka**

Složka NETLOGON je důležitá pro systémy nižší než Windows 2000. Obsahuje například skripty, které se spouštějí při přihlašování uživatele. V systémech Windows 2000/XP/2003 se přihlašovací skripty používají poněkud jiným způsobem a jsou uložené v jiné složce.

## Konfigurace služby DNS na řadiči domény

Služba DNS nyní obsahuje jedinou zónu **studny.local**. Ta je primární zónou s povolenými dynamickými aktualizacemi (viz obrázek 7.12).




**Obrázek 7.12**
Vlastnosti zóny studny.local

Povolení dynamických aktualizací je z pohledu zabezpečení funkce sítě nebezpečné. Teoreticky by se totiž mohlo stát, že by například některý uživatel přejmenoval svůj počítač na SRVR001 a restartoval jej. Po jeho spuštění by došlo k dynamické aktualizaci záznamu SRVR001 na adresu IP onoho klientského počítače, a protože počítač SRVR001 plní v síti celou řadu úloh, byly by všechny úlohy směrované jinam a doména by přestala pracovat.

Je tedy nutné tuto zónu zabezpečit tak, aby se podobné chování zcela vyloučilo nebo alespoň velmi omezilo. Proto postupujte podle následujících pokynů:

1. K počítači **SRVR001** se přihlaste jako správci a spusťte konzolu **DNS**.

**Poznámka**

Správu služby DNS může provádět také uživatel, který není správcem, ale je členem skupiny DnsAdmins. Tato možnost se vyskytuje ve větších prostředích s decentralizovanou správou.

2. Rozbalte položku **Zóny dopředného vyhledávání**, pravým tlačítkem myši klepněte na zónu **studny.local** a z místní nabídky vyberte položku **Vlastnosti**.
3. Na kartě **Obecné** klepněte na tlačítko **Změnit** a poté zaškrtněte políčko **Uložit zónu do adresáře Active Directory (dostupné pouze pokud je server DNS řadičem domény)**. Klepněte na tlačítko **OK** a v dalším dialogovém okně klepněte na tlačítko **Ano**.
4. V rozevíracím seznamu **Dynamické aktualizace** vyberte položku **Pouze zabezpečené** a poté klepněte na tlačítko **OK**.
5. Spusťte aplikaci **Průzkumník Windows** a ve složce **C:\WINDOWS\SYSTEM32\DNS** ověřte, že neexistuje soubor **studny.local.dns**. Informace ze souboru **studny.local.dns** se po změně typu zóny staly součástí doménové databáze Active Directory a soubor se z uvedené cesty přesunul do podsložky **BACKUP**.

## Konfigurace klientských počítačů

Všechny nainstalované klientské počítače je nyní třeba vložit do domény. Postupujte podle následujících pokynů:

1. K počítači **PC001** se přihlaste jako správci.
2. V **Nabídce Start** klepněte pravým tlačítkem myši na položku **Tento počítač** a poté v místní nabídce na položku **Vlastnosti**.
3. Na kartě **Název počítače** klepněte na tlačítko **Změnit** a poté v části **Je členem** zaškrtněte políčko **Domény** a zadejte název **studny.local**. Poté klepněte na tlačítko **OK**.
4. V dialogovém okně **Změny názvu počítače** zadejte jméno **Administrator** a heslo (**K@f!cko**) a klepněte na tlačítko **OK**. V doméně dojde k vytvoření účtu počítače **PC001** a v počítači se zobrazí dialogové okno se zprávou **Vítejte v doméně studny.local**.
5. Postupným klepnutím na všechna tlačítka **OK** a **Ano** provedete restartování počítače.

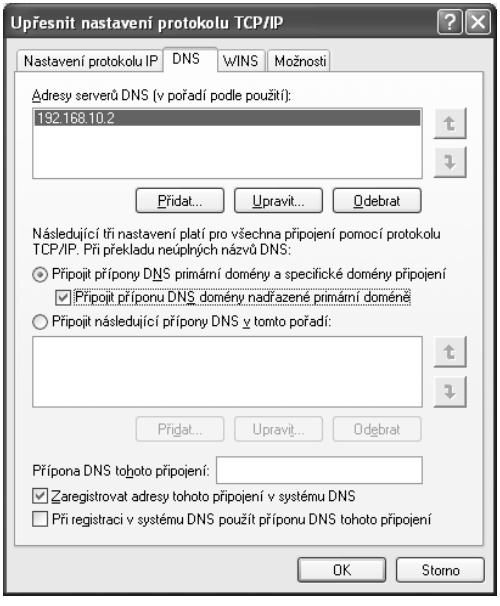
Postup podle bodů 1 až 5 opakujte pro ostatní stanice.

#### Poznámka

Pokud nebude možné vytvořit účet počítače v doméně, bude pravděpodobně problém se službou DNS. V takovém případě postupujte podle následujících pokynů.

1. V **Nabídce Start** klepněte pravým tlačítkem myši na položku **Tento počítač** a poté v místní nabídce klepněte na položku **Vlastnosti**. Na kartě **Název počítače** by měl být v části **Úplný název počítače** zobrazen název **pc00x.studny.local**, kde **pc00x** je název konkrétního počítače. Pokud přípona **studny.local** chybí, můžete ji klepnutím na tlačítko **Změnit** a poté **Další** doplnit do pole **Primární přípona DNS tohoto počítače**. Tento zásah vyžaduje restartování počítače.
2. V **Nabídce Start** klepněte na položku **Ovládací panely**, poté na položku **Připojení k síti a Internetu** a ještě na ikonu **Síťová připojení**. Pravým tlačítkem myši klepněte na položku **Připojení k místní síti** a v místní nabídce zvolte položku **Vlastnosti**.

3. Klepněte na položku **Protokol sítě Internet (TCP/IP)** a poté na tlačítko **Vlastnosti**.
4. Na kartě vlastností protokolu TCP/IP klepněte na tlačítko **Upřesnit** a poté klepněte na kartu **DNS**. Zde ověřte, zda je správně zadaná adresa IP serveru DNS (192.168.10.2) a zda je zaškrtnuté políčko **Připojit přípony DNS primární domény a specifické domény připojení**. Pokud ne, zaškrtněte je. Dialogová okna zavřete postupným klepnutím na tlačítko **OK**.




**Obrázek 7.13**
Správná konfigurace karty DNS

5. Spusťte příkazový řádek a zadejte příkaz `PING studny.local`. Pokud se zobrazí odpovědi, je konektivita počítače do sítě v pořádku a služba DNS pracuje správně.
6. Pokud ani poté nelze přidat počítač do domény, ověřte správnou funkci řadiče domény, případně funkci protokolu TCP/IP pomocí postupů popsaných v kapitole 3, „Učíme počítače komunikovat v síti“.

## Ověření existence účtů počítačů v doméně

1. K počítači **SRVR001** se přihlaste jako správci.
2. V **Nabídce Start** přejděte na položku **Nástroje pro správu** a poté klepněte na nástroj **Uživatelé a počítače služby Active Directory**.
3. V levém podokně tohoto nástroje klepněte na kontejner **Computers**. V pravém podokně by měly být zobrazeny účty počítačů.
4. V levém podokně klepněte na položku **Domain Controllers** a v pravém podokně ověřte existenci účtu řadiče domény **SRVR001**.

**Poznámka**

**Účty řadičů domén jsou v databázi Active Directory z důvodu zabezpečení umístěné ve zvláštní organizační jednotce. Účty z tohoto umístění nepřesunujte!**

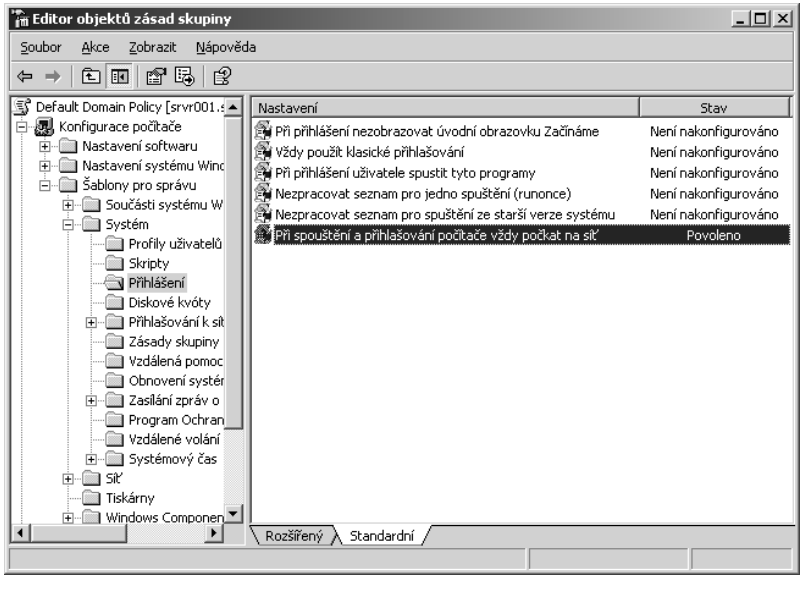
# Konfigurace přihlášení k počítači

Systémy Windows XP i serverové operační systémy řady Windows Server 2003 se spouštějí rychleji než předchůdci Windows 2000. To není dáno tím, že by jádro systému bylo výrazně pozměněno a spuštění počítače bylo opravdu rychlejší. Jednoduše se pro přihlášení uživatele nečeká na spuštění sítě.

Takový stav jistě mnoha milionům zejména domácích uživatelů na světě vyhovuje, neboť své počítače v síti nemají (a společnosti Microsoft tiše děkují, že systémy Windows XP Professional a Windows Server 2003 obsahují konečně vylepšení viditelné na první pohled). V prostředí organizace, která síť používá, to však není úplně nejlepší nastavení, protože naopak někdy může zbrzdit přenesení informací k uživateli až na druhé přihlášení.

Tuto funkci lze vypnout a vzhledem k tomu, že v prostředí domény je žádoucí, aby síť pracovala ještě před přihlášením uživatele k počítači, doporučuji tuto vlastnost zakázat podle následujícího postupu:

1. Přihlaste se k serveru **SRVR001** jako správci.
2. V **Nabídce Start** přejděte na položku **Nástroje pro správu** a poté klepněte na položku **Uživatelé a počítače služby Active Directory**.
3. Pravým tlačítkem myši klepněte na položku domény (**studny.local**) a v místní nabídce klepněte na položku **Vlastnosti**. Zobrazí se dialogové okno vlastností domény.
4. Na kartě **Zásady skupiny** poklepejte na položku **Default Domain Policy**. Zobrazí se konzola **Editor objektů zásad skupiny**.
5. V levém podokně konzoly v části **Konfigurace počítače** rozbalte položku **Šablony pro správu**, poté položku **Systém** a klepněte na položku **Přihlášení**.
6. V pravém okně poklepejte na položku **Při spouštění a přihlašování počítače vždy počkat na síť** a zaškrtněte políčko **Povoleno**. Poté klepněte na tlačítko **OK**.




**Obrázek 7.14** Zásada v objektu na úrovni domény

**Poznámka**

**Uvedené nastavení se týká pouze počítačů se systémy Windows XP Professional a systémů řady Windows Server 2003. Systémy Windows 2000 se standardně chovají tak, jako by toto nastavení bylo vždy povolené (vždy čekají nejprve na síť).**

# Závěr

Doména Active Directory přišla v porovnání se svým předchůdcem, doménou SAM se systémem Windows NT 4.0 Server, s mnoha vylepšeními. Ta se týkají možnosti uložení řádově většího množství objektů (uživatelské účty, účty počítačů, skupiny apod.), možností delegování správy pro větší prostředí s více správci nebo například zabezpečení.

Přesto se vyskytují prostředí, pro která je jediná doména nedostatečná. Jde spíše o větší společnosti s pobočkami po celém světě nebo například o společnosti, které se nedávno spojily s jinou organizací. V jejich doménové struktuře můžete najít více domén, které mohou být uspořádané ve formě stromu či lesa Active Directory.

Strom Active Directory sdružuje jednu či více domén, jejichž názvy jsou souvislé. Stromová struktura je hierarchická, tato hierarchie se však týká pouze názvů. Rozhodně to tedy neznamená, že správci nadřazené domény mohou automaticky spravovat podřízené domény. Nejvyšší privilegia má sice ta doména, která byla nainstalovaná jako první, všechny ostatní domény jsou si z pohledu správy rovny.

Někdy je však nutné (například při splynutí dvou organizací) ponechat každé původní doméně vlastní název. Řešením jsou v takovém případě dva stromy (jinak nelze zajistit nesouvislost názvů domén) sdružené v jednom lese.

Při instalaci domény je nutné dobře zvolit její název, neboť od něj se odvíjí názvy případných dalších domén. Dále instalace domény vyžaduje službu DNS. Pokud v síti existuje, vytvoří se v zóně se stejným názvem, jako má doména, nové záznamy SRV určující umístění jednotlivých doménových služeb. Pokud zóna se stejným názvem neexistuje nebo pokud v síti vůbec neexistuje služba DNS, nabídne Průvodce instalací domény konfiguraci služby DNS. V takovém případě dojde k instalaci služby DNS a její konfiguraci na řadič domény.

Instalace domény znamená úplnou změnu prostředí sítě. Proto je třeba se na tuto situaci dobře připravit, neboť pozdější změny v doméně mohou mít vliv na všechny počítače v síti.

## Stav sítě

V této kapitole došlo k největší změně v naší síti. Model pracovní skupiny byl změněn na doménu Active Directory. Počítač SRVR001 se stal řadičem domény a všechny klientské počítače členy domény. Na závěr jsme nakonfigurovali zásadu, která zakáže všem uživatelům v doméně možnost přihlásit se dříve, než dojde ke spuštění síťových součástí. Toto chování, které je nyní stejné jako u systémů Windows 2000, je vhodné do doménových prostředí, neboť správci mají jistotu, že vše v doméně pracuje ihned tak, jak určili.