KAPITOLA 7

Použití služby Active Directory

V této kapitole:

Adresářová služba Active Directory Domain Services je rozšiřitelná a škálovatelná adresářová služba, kterou můžete použít k efektivnímu uspořádání síťových prostředků. Jako správci musíte vědět, jak služba Active Directory pracuje. Potřebné informace k tomu naleznete v této kapitole. Pokud jste dříve s technologií Active Directory nepracovali, jistě si okamžitě všimnete, že je poměrně velmi pokročilá a nabízí mnoho funkcí. Dále se podíváme na přehled služby Active Directory a poté se zaměříme na její součásti.

Úvod do služby Active Directory

Služba Active Directory je srdcem domén založených na systému Windows už od dob svého představení v systému Windows 2000. Téměř každá úloha správy, kterou provedete, nějakým způsobem službu Active Directory ovlivní. Služba Active Directory je založena na standardních internetových protokolech a je navržena tak, aby umožnila jednoznačně definovat strukturu sítě.

Služby Active Directory a DNS

Služba Active Directory využívá službu DNS (Domain Name System). Služba DNS je standardní internetovou službou, která organizuje skupiny počítačů do domén. Struktura domén služby DNS je hierarchická. Hierarchie domén služby DNS je založena na prostředí Internetu. Rozdílné úrovně v hierarchii určují počítače, domény organizací a domény nejvyšší úrovně. Služba DNS se také používá k mapování hostitelských názvů, například zeta.microsoft.com, k adresám protokolu TCP/IP (Transmission Control Protocol/Internet Protocol), například 192.168.19.2. Prostřednictvím služby DNS může být hierarchie domén Active Directory také definována na základech Internetu nebo může být samostatná a neveřejná.

Při hledání počítačů v tomto typu domény se používají plně kvalifikované názvy domény (Fully Qualified Domain Name, FQDN), jako např. zeta.microsoft.com. *Zeta* zde představuje název příslušného počítače, *microsoft* představuje doménu organizace a *com* je doména nejvyšší úrovně. Domény nejvyšší úrovně jsou základem hierarchie služby DNS, a nazývají se proto *kořenové domény.* Tyto domény jsou zeměpisně rozdělené pomocí dvoupísmenných kódů zemí, například kód CA je pro Kanadu, typem organizace, například *com* pro komerční organizace, a funkcí, například *mil* pro vojska Spojených států.

Běžné domény, například microsoft.com, se také označují jako *nadřazené domény*. Nazývají se tak proto, že jsou nadřazeny organizační struktuře. Nadřazené domény mohou být rozděleny do poddomén, které lze využívat v různých kancelářích, divizích nebo zeměpisných lokalitách. Například plně kvalifikovaný název domény počítače v kanceláři společnosti Microsoft v Seattlu může být jacob.seattle.microsoft.com. V tomto případě je *jacob* názvem počítače, *seattle* je poddoména a *microsoft.com* je nadřazená doména. Dalším výrazem pro poddoménu je *podřízená doména*.

Služba DNS je natolik nedílnou součástí služby Active Directory, že je nutné ji v síti nakonfigurovat ještě před instalací služby Active Directory. Práce se službou DNS je popsána v kapitole 20, „Optimalizace služby DNS".

V případě systému Windows Server 2008 probíhá instalace služby Active Directory ve dvou fázích. Nejprve na server přidáte pomocí Průvodce přidáním role (Add Role Wizard) roli Služba AD DS (Active Directory Domain Services). Poté spustíte Průvodce instalací služby Active Directory (Active Directory Installation Wizard). Klepněte na tlačítko Start, do pole Hledat (Search) zadejte příkaz **dcpromo** a poté stiskněte klávesu Enter. Jestliže není nainstalována služba DNS, budete vyzváni k jejímu nainstalování. Pokud doména neexistuje, průvodce ji vytvoří a nakonfiguruje službu Active Directory v nové doméně. Průvodce rovněž může přidat do existujících doménových struktur podřízené domény. Pro ověření korektnosti instalace řadiče domény můžete:

- Zkontrolovat chyby v protokolu událostí adresářové služby.
- Ujistit se, že klienti mají přístup ke složce Sysvol.
- Ověřit, zda služba DNS umožňuje překlad názvů.
- Ověřit replikaci změn na adresář Active Directory.

Poznámka: V další části této kapitoly se často vyskytují termíny adresář a domény, kterými se označuje služba Active Directory a domény služby Active Directory. Výjimkou je, když je třeba rozlišit struktury služby Active Directory od služby DNS nebo od jiných typů adresářů.

Instalace řadičů domény jen pro čtení

Jak již bylo zmíněno v kapitole 1, „Přehled správy systému Windows Server 2008", řadiče domény se systémem Windows Server 2008 mohou být nakonfigurovány jako

řadiče domény jen pro čtení. Pokud na řadič domény jen pro čtení nainstalujete službu DNS Server, tento řadič domény jen pro čtení může sloužit jako server DNS jen pro čtení. Při této konfiguraci platí následující podmínky:

- Řadič domény jen pro čtení replikuje aplikační oddíly adresáře, které server DNS používá, včetně oddílů ForestDNSZones a DomainDNSZones. Klienti mohou položit dotaz serveru DNS jen pro čtení na překlad názvu. Ovšem server DNS jen pro čtení nepodporuje přímou aktualizaci klientů, neboť server DNS jen pro čtení neregistruje záznamy o prostředcích pro všechny zóny integrované ve službě Active Directory, které hostí.
- Pokud se klient pokusí aktualizovat své záznamy DNS, server vrátí odkaz. Klient se poté může pokusit o aktualizaci oproti serveru DNS, který je uveden v odkazu. Prostřednictvím replikace na pozadí se server DNS jen pro čtení pokusí přijmout aktualizovaný záznam od serveru DNS, který aktualizaci provedl. Tento požadavek na replikaci slouží pouze pro změněný záznam DNS. Úplný seznam změněných dat zón nebo domény se během tohoto speciálního požadavku nereplikuje.

Prvním řadičem domény se systémem Windows Server 2008, nainstalovaným v doménové struktuře nebo v doméně, nemůže být řadič domény jen pro čtení. Ovšem další řadiče domény můžete nakonfigurovat jen pro čtení. Pro účely plánování mějte na paměti následující skutečnosti:

- Před prvním přidáním služby Active Directory Domain Services (AD DS) na server se systémem Windows Server 2008 v doménové struktuře se systémem Windows Server 2003 nebo Windows 2000 Server musíte aktualizovat schéma v hlavním operačním schématu serveru v doménové struktuře spuštěním příkazu adprep/ /forestprep.
- Před prvním přidáním služby AD DS na server se systémem Windows Server 2008 v doméně se systémem Windows Server 2003 nebo Windows 2000 Server musíte aktualizovat hlavní server infrastruktury v doméně spuštěním příkazu adprep/ /domainprep /gpprep.
- Před instalací služby AD DS, a tím vytvořením vašeho prvního řadiče domény jen pro čtení v doménové struktuře, musíte připravit doménovou strukturu spuštěním příkazu adprep/rodcprep.

Systém Windows Server 2008 se systémem Windows NT 4.0

Doménové funkce systému Windows Server 2008 nejsou navrženy tak, aby spolupracovaly s doménovými funkcemi systému Windows NT 4.0. Řadiče domény se systémem Windows NT Server 4.0 nejsou v systému Windows Server 2008 podporovány. Kvůli těmto problémům při spolupráci byste měli učinit následující opatření:

- Aktualizovat řadiče domény se systémem Windows NT Server 4.0 před instalací všech počítačů se systémem Windows Server 2008.

- Aktualizovat všechny počítače se systémem Windows NT Server 4.0 před instalací všech řadičů domény se systémem Windows Server 2008.

Systém Windows NT Server 4.0 můžete upgradovat na systém Windows 2000 Server nebo Windows Server 2003. Důležité je zapamatovat si, že při provádění upgradu všech počítačů se systémem Windows NT Server 4.0 je stále vyžadován hlavní operační server pro emulaci primárního řadiče domény.

Práce s doménovými strukturami

Služba Active Directory obsahuje logické i fyzické struktury součástí sítě. Logické struktury pomáhají při organizaci objektů adresářové služby a při správě účtů a sdílených prostředků sítě. Mezi logické struktury patří:

- **Organizační jednotky (Organization Unit)** – podskupina domény, která často odpovídá obchodní nebo funkční struktuře organizace.
- **Domény (Domain)** – skupina počítačů sdílejících společnou adresářovou databázi.
- **Stromy domén (Forest)** – jedna nebo více domén sdílejících souvislý obor názvů.
- **Doménové struktury domén (Domain Tree)** – jeden nebo více stromů domén sdílejících společné adresářové informace.

Fyzické struktury usnadňují komunikaci v síti a fyzicky ohraničují prostředky sítí. Mezi fyzické struktury, které vám mohou pomoci mapovat fyzickou strukturu sítě, patří:

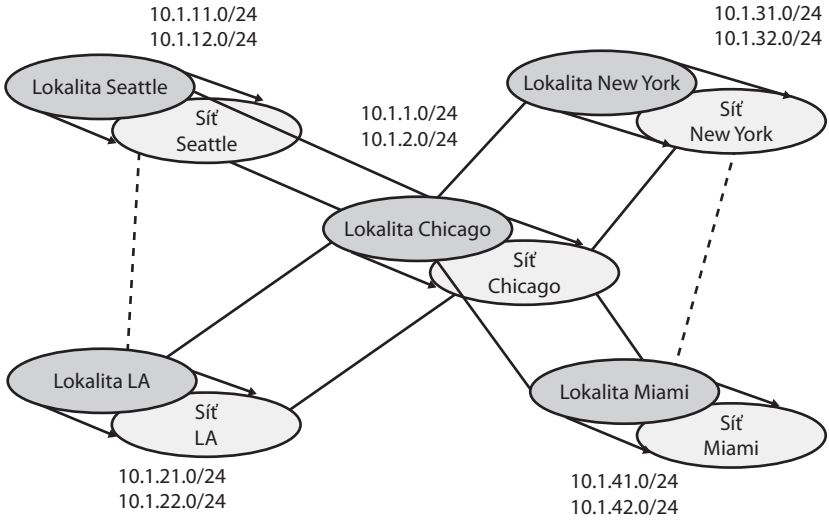
- **Podsítě (Subnets)** – síťová skupina se specifickým rozsahem adres IP a masky podsítě.
- **Sítě (Site)** – jedna nebo více podsítí; slouží ke konfiguraci přístupu k adresářové službě a replikací.

Domény

Doména Active Directory je jednoduše skupinou počítačů sdílejících společnou adresářovou databázi. Názvy domén Active Directory musí být jedinečné. Nemůže mít například dvě domény microsoft.com, ale k nadřazené doméně microsoft.com může mít podřízené domény, jako např. seattle.microsoft.com nebo ny.microsoft.com. Pokud je taková doména součástí privátní sítě, nesmí být název nové domény v konfliktu s žádným jiným existujícím názvem domény v této síti. Pokud je doména součástí sítě Internet, nesmí být její název v konfliktu se žádným názvem domény, která existuje v síti Internet. Abyste zajistili jedinečnost názvu v síti Internet, musíte zaregistrovat název nadřazené domény předtím, než jej začnete používat. Registrace domény se může provést prostřednictvím jakéhokoli určeného registrátora. Aktuální seznam určených registrátorů naleznete na internetové adrese organizace InterNIC (*http://www.internic.net*).

Každá doména má své vlastní zásady zabezpečení a vytvořený vztah důvěryhodnosti s ostatními doménami. Domény mohou také zahrnovat více fyzických míst, takže se doména může skládat z více sítí, které mohou mít více podsítí, jak vidíte na obrázku 7.1.

V adresářové databázi domény naleznete současně s objekty určující účty uživatelů, skupin a počítačů a také sdílené prostředky, jako například tiskárny nebo složky.



Obrázek 7.1: Síťový diagram pro rozsáhlou síť WAN se spoustou lokalit a podsítí

Poznámka: Bližší informace o uživatelských a skupinových účtech naleznete v kapitole 9, „Základy uživatelských a skupinových účtů". Bližší informace o účtech počítačů a různých typech počítačů používaných v doménách operačního systému Windows Server 2008 naleznete dále v části „Práce s doménami Active Directory".

Funkce domény jsou omezeny a určeny úrovní funkčnosti domény. K dispozici jsou některé další úrovně funkčnosti domény, mezi které patří:

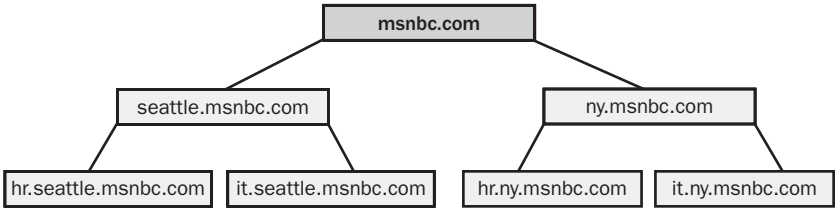
- **Windows 2000 mixed** – podporuje řadiče domény se systémy Windows NT 4.0 a novější verze systému Windows Server. Ovšem řadiče domén se systémem Windows NT 4.0 nelze použít se systémem Windows Server 2008 a řadiče domén se systémem Windows Server 2008 nelze použít se servery se systémem Windows NT 4.0.
- **Windows 2000 native** – podporuje řadiče domény se systémy Windows 2000 a novějšími verzemi systému Windows.
- **Windows Server 2003** – podporuje řadiče domény se systémy Windows Server 2003 a Windows Server 2008.
- **Windows Server 2008** – podporuje řadiče domény se systémem Windows Server 2008.

Další informace týkající se úrovně funkčnosti domén naleznete dále v této kapitole v části „Práce s úrovněmi funkčnosti domén".

Doménové struktury a stromy domén

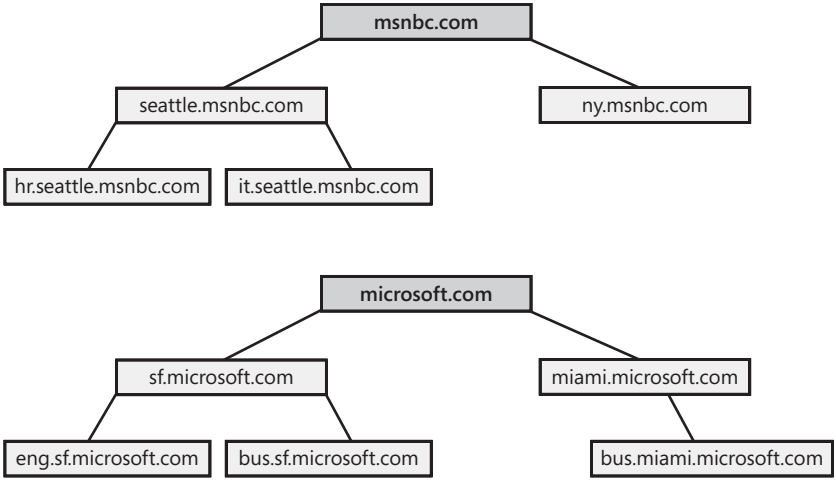
Každá doména služby Active Directory má název domény DNS, jako například microsoft.com. Jedna nebo více domén sdílejících stejná adresářová data se nazývají *doménová struktura*. Názvy domén v této doménové struktuře mohou být z pohledu hierarchie názvů DNS *nesouvislé* nebo *souvislé*.

Pokud mají domény souvislou strukturu názvů, jsou součástí stejného *stromu domén*. Příklad doménového stromu je uveden na obrázku 7.2. V tomto případě má kořenová doména msnbc.com dvě podřízené domény – seattle.msnbc.com a ny.msnbc.com. Tyto domény mají další poddomény. Všechny tyto domény jsou součástí stejného stromu, protože mají společnou kořenovou doménu.



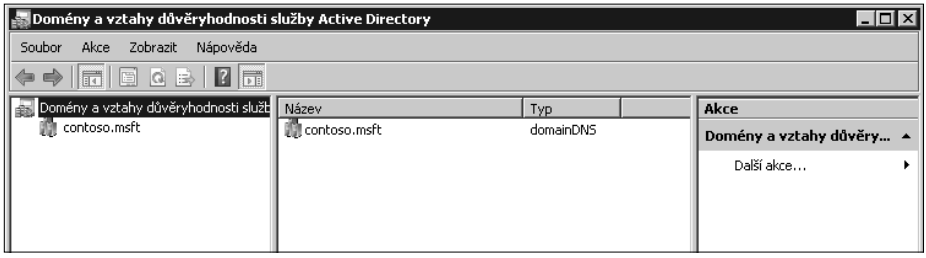
Obrázek 7.2: Domény ve stejném stromu sdílejí souvislou strukturu názvů

Pokud mají domény v doménové struktuře nesouvislé názvy domény DNS, vytvářejí samostatné stromy domén v rámci doménové struktury. Jak je zřejmé z obrázku 7.3, doménová struktura může mít jeden nebo více stromů domén. V tomto případě vytvářejí domény msnbc.com a microsoft.com kořeny samostatných doménových stromů ve stejné doménové struktuře.



Obrázek 7.3: Více stromů v doménové struktuře má nesouvislé struktury názvů

Strukturu domén je možné zobrazit pomocí nástroje Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts), jak ukazuje obrázek 7.4. Nástroj Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts) je modulem snap-in konzoly MMC (Microsoft Management Console), který lze rovněž spustit prostřednictvím nabídky Nástroje pro správu (Administrative Tools). Každá kořenová doména zde má vlastní záznam. Kořenovou doménou na obrázku je doména s názvem cpandl.com.



Obrázek 7.4: Pro práci s doménami, doménovými strukturami a stromy používejte nástroj Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts)

Funkce doménové struktury jsou určeny a omezeny funkční úrovní doménové struktury. K dispozici je několik funkčních úrovní doménové struktury:

- **Windows 2000** – podporuje řadiče domény se systémy Windows NT 4.0 a novější verze systému Windows Server. Ovšem řadiče domén se systémem Windows NT 4.0 nelze použít se systémem Windows Server 2008 a řadiče domén se systémem Windows Server 2008 nelze použít se servery se systémem Windows NT 4.0.
- **Windows Server 2003** – podporuje řadiče domény se systémy Windows Server 2003 a Windows Server 2008.
- **Windows Server 2008** – podporuje řadiče domény se systémem Windows Server 2008.

Funkční úroveň doménové struktury Windows Server 2003 nabízí podstatné zlepšení výkonu služby Active Directory a funkcí oproti funkční úrovni doménové struktury Windows 2000. Pokud v tomto režimu pracují všechny domény stejné doménové struktury, dojde také ke zlepšení replikace globálního katalogu a účinnosti replikace dat služby Active Directory. Protože se replikují také hodnoty připojení, můžete rovněž zaznamenat zlepšení replikace mezi sítěmi. Budete moci deaktivovat objekty tříd a atributů schématu, používat dynamické pomocné třídy, přejmenovávat domény a vytvářet vlastní jednosměrné nebo obousměrné a přenosné vztahy důvěryhodnosti mezi doménovými strukturami.

Funkční úroveň doménové struktury Windows Server 2008 nabízí podstatné zlepšení výkonu služby Active Directory a funkcí oproti funkční úrovni doménové struktury Windows 2003. Pokud v tomto režimu pracují všechny domény stejné doménové struktury, získáme vylepšenou replikaci mezi lokalitami i v rámci lokalit celé organizace. Také řadiče domény budou místo replikace pomocí služby FRS používat replikaci pomocí služby DFS. A zaregistrované objekty zabezpečení systému Windows Server 2008 se

nevytvoří, pokud hlavní operační server pro emulaci primárního řadiče domény v kořenové doméně adresářové struktury neběží se systémem Windows Server 2008. Tento požadavek je podobný požadavku u systému Windows Server 2003.

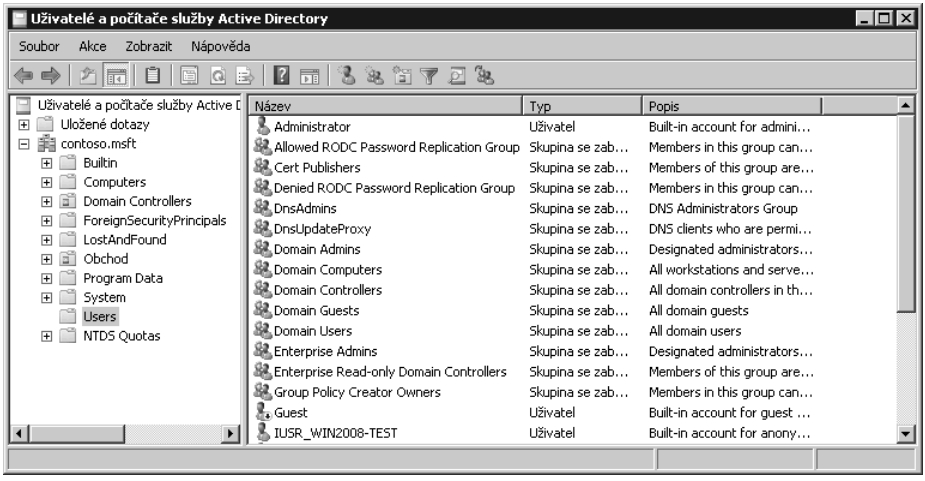
Organizační jednotky

Organizační jednotky jsou podskupiny v rámci domén, které často odrážejí řídicí nebo obchodní strukturu organizace. Organizační jednotky si také můžete představit jako logické kontejnery, do kterých je možné umístit účty, sdílené prostředky a další organizační jednotky. V doméně microsoft.com můžete například vytvořit organizační jednotky se jménem LidskeZdroje, IT, Vyvoj a Marketing. Později můžete toto schéma rozšířit přidáním podřízených jednotek. Podřízené organizační jednotky Marketing by mohly mít názvy ProdejOnline, DistribucniProdej a PrimyProdej.

Objekty umístěné v jedné organizační jednotce mohou vycházet pouze z nadřazené domény. Například organizační jednotky domény seattle.microsoft.com mohou obsahovat objekty pouze z této domény. Není možné do nich přidávat například žádné objekty z domény ny.microsoft.com.

Organizační jednotky jsou velmi užitečné pro uspořádání objektů obchodní nebo řídicí struktury organizace. Stále to ale není jediný důvod, proč organizační jednotky používat. Mezi další důvody patří:

- Organizační jednotky umožňují přiřadit zásady skupiny pro malý počet objektů domény, aniž by tyto zásady ovlivňovaly zbytek domény. To umožňuje stanovit a spravovat zásady skupiny na patřičné úrovni společnosti.



Obrázek 7.5: Správu uživatelů, skupin, počítačů a organizačních jednotek provádějte pomocí nástroje Uživatelé a počítače služby Active Directory (Active Directory Users And Computers)

- Organizační jednotky vytvářejí menší pohledy na adresářové objekty domény a je tak možné s nimi lépe pracovat. To umožňuje efektivnější správu prostředků.
- Organizační jednotky umožňují delegovat řízení a jednoduše řídit přístup ke správě doménových prostředků. Máte tak možnost řídit rozsah práv správce v doméně. Uživateli A můžete udělit oprávnění správce platná pro jednu organizační jednotku a ne pro ostatní. Stejně můžete udělit uživateli B oprávnění správce platná pro všechny organizační jednotky v této doméně.

Organizační jednotky jsou v nástroji Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) reprezentované složkami (viz obrázek 7.5). Tento nástroj je modulem snap-in konzoly MMC (Microsoft Management Console), který můžete spustit rovněž pomocí nabídky Nástroje pro správu (Administrative Tools).

Sítě a podsítě

Síť je skupinou počítačů sestávající z jedné nebo více podsítí protokolu IP. Jsou určené k reprezentaci fyzické struktury sítě. Sítě jsou nezávislé na logických doménových strukturách a nemají proto spolu žádný vztah. V jedné doméně Active Directory je možné vytvářet více sítí nebo můžete mít jednu síť, která bude k dispozici více doménám. Mezi rozsahem adres IP používaných v síti a oborem názvů domén rovněž neexistuje žádná souvislost.

Podsíť si můžete představit jako skupinu síťových adres. Na rozdíl od sítí, které mohou mít více rozsahů adres IP, mají podsítě specifický rozsah adres IP a masku podsítě. Názvy podsítí jsou uvedeny ve formátu *síť/počet bitů masky*, jako například 192.168.19.0/24. V tomto případě vytváří adresa 192.168.19.9 a maska podsítě 255.255.255.0 kombinaci 192.168.19.0/24.

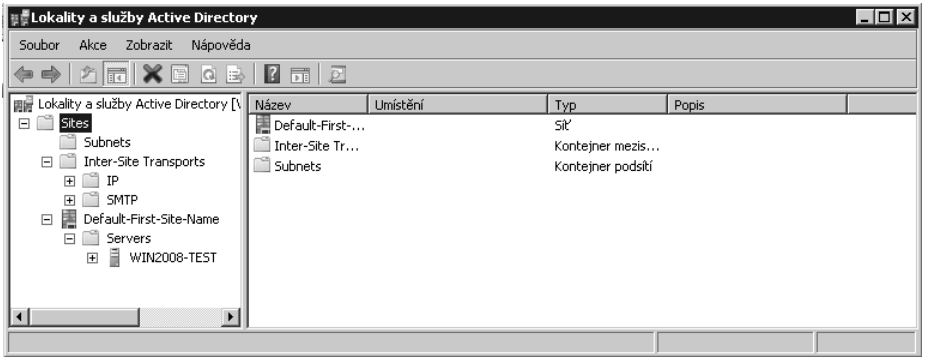
Poznámka: Nemusíte vědět, jak se vytváří označení podsítě. Ve většině případů zadáte síťovou adresu a masku podsítě a systém Windows Server 2008 poté vygeneruje její označení.

Počítače jsou zařazeny do sítí na základě jejich umístění v podsíti. Pokud mohou počítače spolu v podsíti efektivně komunikovat, říkáme, že mají *rychlé spojení*. V ideálním případě se sítě skládají z podsítí a počítačů s rychlým spojením. Pokud nemají počítače v podsítích rychle spojení, bude možná nutné vytvořit více sítí. Rychlé spojení připojení přináší sítím několik výhod:

- Když se klientské počítače přihlásí k doméně, proces ověření nejprve vyhledá řadiče domény, které jsou ve stejné síti jako počítač. Znamená to, že pokud je to možné, použijí se místní řadiče jako první, ověření proběhne místně a jako takové se urychlí.
- Adresářová informace se častěji replikuje v rámci sítě než mezi sítěmi. Tím se snižuje zatížení sítě způsobené replikacemi a zároveň se zajistí, že místní řadiče domény

mají k dispozici nejnovější informace. Pomocí spojení sítí (site links) také můžete sami určit, jak se budou adresářové informace replikovat. Řadič domény, používaný k replikaci mezi sítěmi, se nazývá *bridgehead server*. Tím se veškeré vytížení týkající se replikací mezi sítěmi přenese na jediný server namísto zatěžování ostatních.

Sítě a podsítě se spravují pomocí nástroje Sítě a služby Active Directory (Active Directory Sites And Services) tak, jak je uvedeno na obrázku 7.6. Protože se jedná o modul snap-in, můžete jej přidat do jakékoli konzoly. Nástroj Sítě a služby Active Directory (Active Directory Sites And Services) můžete otevřít z nabídky Nástroje pro správu (Administrative Tools).



Obrázek 7.6: Ke správě sítí a podsítí slouží nástroj Sítě a služby Active Directory (Active Directory Sites And Services)

Práce s doménami Active Directory

Přestože v síti se systémem Windows Server 2008 musí být nakonfigurovány služby Active Directory i DNS (Domain Name System), mají domény Active Directory a domény DNS jiný účel. Domény Active Directory slouží ke správě účtů, prostředků a zabezpečení. Domény DNS zavádějí hierarchii domén, která se primárně používá pro překlad názvů. Systém Windows Server 2008 využívá službu DNS k mapování hostitelských názvů, jako například zeta.microsoft.com k adrese IP, jako například 172.16.18.8. Další informace o službě DNS a doménách DNS naleznete v kapitole 20.

Počítače se systémem Windows 2000 a novějším v doméně Active Directory

Uživatelské počítače s profesionálními nebo business edicemi systémů Windows 2000, Windows XP a Windows Vista mohou službu Active Directory plně využívat. Přistupují k síti jako klienti služby Active Directory a plně využívají jejích funkcí. Jako klienti mohou využívat přenosné vztahy důvěryhodnosti, které existují v rámci stromu nebo

doménové struktury. Přenosná důvěryhodnost je ta, která není explicitně stanovena. Vytváří se automaticky na základě struktury a povolení nastavených v rámci doménové struktury. Takové vztahy umožňují ověřeným uživatelům přistupovat k prostředkům jakékoli domény v doménové struktuře.

Serverové počítače se systémy Windows 2000 Server, Windows Server 2003 a Windows Server 2008 poskytují služby ostatním systémům a mohou se chovat jako řadiče domény nebo členské servery. Řadič domény se liší od členského serveru tím, že je v něm spuštěná služba Active Directory Domain Services. Členské servery lze na řadiče domény povýšit instalací služby Active Directory Domain Services. Odinstalováním služby Active Directory Domain Services snížíte úroveň řadičů domény zpět na členské servery. Pro přidání nebo odebrání služby Active Directory Domain Services použijte Průvodce přidáním rolí (Add Role Wizard) a Průvodce odebráním rolí (Remove Role Wizard). Zvýšení nebo snížení úrovně serveru se provádí pomocí Průvodce instalací služby Active Directory (Active Directory Installation Wizard) (dcpromo.exe).

Domény mohou mít jeden nebo více řadičů domény. Pokud existuje více řadičů, replikují si automaticky mezi sebou data adresářové služby pomocí replikace typu multimaster. Tento model umožňuje jakémukoli řadiči domény zpracovat adresářové změny a poté je replikovat na ostatní řadiče domény.

Vzhledem ke struktuře domény typu multimaster mají všechny řadiče domény standardně stejnou odpovědnost. Přesto můžete některým doménovým řadičům udělit pro určité úkoly přednost před ostatními, například specifikací bridgehead serveru, který má prioritu při replikaci adresářových informací do ostatních sítí. Některé úkoly je nejvhodnější provádět pomocí jediného serveru. Takovému serveru se říká *hlavní operační server*. Existuje pět různých rolí hlavních operačních serverů, z nichž každou můžete přidělit jinému řadiči domény. Další informace naleznete v části „Role operačních serverů“ dále v této kapitole.

Všechny počítače se systémy Windows 2000, Windows XP Professional, Windows Vista, Windows Server 2003 a Windows Server 2008, které jsou součástí domény, mají svůj účet. Stejně jako ostatní zdroje jsou také účty počítačů uložené ve formě objektů v doméně Active Directory. Účty počítačů se používají ke správě přístupů k síti a ke zdrojům sítě. Počítač přistupuje k doméně pomocí svého účtu, který je před umožněním přístupu ověřen.

Z praxe: Řadiče domény využívají při ověření počítače i uživatele globální katalog služby Active Directory. Pokud není globální katalog k dispozici, do domény se mohou přihlásit pouze členové skupiny Domain Admins. Důvodem je, že informace o členství v univerzálních skupinách jsou uloženy v globálním katalogu a tato informace je nutná pro ověření. V systému Windows Server 2003 a Windows Server 2008 máte možnost ukládat členství v univerzálních skupinách do místní mezipaměti, čímž se tento problém vyřeší. Další informace naleznete v části „Základy struktury adresářové služby“ dále v této kapitole.

Práce s úrovněmi funkčnosti domény

Všechny počítače se systémy Windows NT, Windows XP, Windows Vista, Windows Server 2003 a Windows Server 2008 musí mít před připojením v doméně účet. Služba Active Directory má pro podporu struktur domén několik úrovní funkčnosti domény:

- **Smíšený režim Windows 2000** – použití tohoto režimu není doporučeno pro systém Windows Server 2008. Nebudete moci použít řadiče domény se systémem Windows Server 2008 a počítače se systémem Windows Server 2008 mohou mít problémy při práci s řadiči domény se systémem Windows NT. Domény fungující v tomto režimu nemohou využít mnoho nových funkcí služby Active Directory, včetně univerzálních skupin, vnořování skupin, převodů typů skupin, snadné přejmenování řadičů domény, aktualizace časových razítek přihlášení a verze klíčů služby distribuce klíčů modulu Kerberos (KDC).
- **Nativní režim Windows 2000** – pracuje-li doména v nativním režimu Windows 2000, adresář podporuje řadiče domény se systémy Windows Server 2008, Windows 2003 a Windows 2000. Řadiče domény se systémem Windows NT nejsou nadále podporovány. Domény v tomto režimu nemohou využívat funkce snadného přejmenování řadičů domény, aktualizace časových razítek přihlášení a verze klíčů služby distribuce klíčů modulu Kerberos (KDC).
- **Windows Server 2003** – pracuje-li doména v režimu Windows 2003, adresář podporuje řadiče domény se systémy Windows Server 2008 a Windows Server 2008. Řadiče domény se systémem Windows NT a Windows 2000 nejsou nadále podporovány. Doména pracující v režimu Windows Server 2003 může využívat mnoho nových funkcí služby Active Directory, včetně univerzálních skupin, vnořování skupin, převodů typů skupin, snadné přejmenování řadičů domény, aktualizace časových razítek přihlášení a verze klíčů služby distribuce klíčů modulu Kerberos (KDC).
- **Windows Server 2008** – pracuje-li doména v režimu Windows Server 2008, adresář podporuje pouze řadiče domény se systémem Windows Server 2008. Řadiče domény se systémem Windows NT, Windows 2000 a Windows Server 2003 nejsou nadále podporovány. Ovšem dobrou zprávou je, že doména pracující v režimu Windows Server 2003 může využívat všechny nové funkce služby Active Directory, mezi které patří služba Replikace distribuovaného systému souborů (DFS Replication) pro vylepšenou replikaci mezi lokalitami i v rámci lokalit.

Nativní režim Windows 2000

Po upgradu primárního řadiče domény, záložních řadičů domény a ostatních počítačů se systémy Windows NT, můžete v případě, že máte stále prostředky domény se systémem Windows 2000, přepnout doménu do nativního režimu Windows 2000 a poté v doméně používat pouze systémy Windows 2000, Windows Server 2003 a Windows Server 2008. V okamžiku, kdy režim přepnete do nativního systému Windows 2000, se už nebudete moci vrátit ke smíšenému režimu. Proto byste měli používat nativní

režim pouze tehdy, pokud budete mít jistotu, že nebudete původní strukturu domény se systémy Windows NT nebo záložní řadiče domény se systémem Windows NT potřebovat.

Po změně režimu na nativní režim Windows 2000 dojde k následujícím změnám možností:

- Upřednostňovaným ověřovacím mechanismem se stane protokol Kerberos V5 a ověřování NTLM se nebude nadále používat.
- Emulátor primárního řadiče domény (PDC emulator) neprovádí synchronizaci s žádným záložním řadičem domény se systémem Windows NT.
- Do domény není možné přidat řadič domény se systémem Windows NT.

Ze smíšeného režimu Windows Server 2000 se můžete přepnout do nativního režimu Windows 2000 zvýšením úrovně funkčnosti domény.

Režim Windows Server 2003

Po provedení upgradu systémů Windows NT ve vaší organizaci můžete pokračovat upgradem na systémy Windows Server 2003. To provedete jako upgrade řadičů domény se systémem Windows 2000 na řadiče domény se systémem Windows Server 2003 nebo Windows Server 2008 a poté, pokud to bude zapotřebí, můžete změnit úroveň funkčnosti na podporu režimu Windows Server 2003.

Před aktualizací řadičů domény se systémem Windows 2000 byste měli nejprve připravit doménu pro provedení upgradu. Abyste tuto operaci mohli provést, budete muset aktualizovat doménovou strukturu a schéma domény tak, aby byly kompatibilní s doménami se systémem Windows Server 2003. K automatickému provedení aktualizace je možné použít nástroj Adprep.exe. Ten stačí spustit na hlavním operačním serveru schématu v doménové struktuře a poté na hlavním operačním serveru infrastruktury v každé doméně doménové struktury. Jako vždy byste měli tyto postupy nejprve ověřit v laboratorním prostředí. Nástroj Adprep najdete v podsložce i386 na instalačním médiu se systémem Windows Server 2003.

Poznámka: Abyste určili, který server je aktuálním hlavním operačním serverem schématu domény, zadejte v příkazovém řádku příkaz dsquery server -hasfsmo schema. Zobrazí se řetězec s názvem serveru, jako například: „CN=CORPSERVER01,CN=Servers, CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=microsoft, DC=com“. Tento řetězec označuje, že hlavní operační server schématu má v doméně microsoft.com název CORPSERVER01.

Poznámka: Abyste určili, který server v doméně je hlavním operačním serverem infrastruktury dané domény, zadejte na příkazovém řádku příkaz dsquery server -hasfsmo infr.

Po provedení upgradu vašich serverů můžete zvýšit úroveň funkčnosti domény a doménové struktury, abyste mohli využívat nejnovější funkce služby Active Directory. Pokud

to provedete, budete moci v doméně používat pouze prostředky systémů Windows Server 2003 a Windows Server 2008 a nebudete se moci vrátit k žádnému předchozímu režimu. Proto byste měli režim Windows Server 2003 použít pouze tehdy, pokud si budete jisti, že již nebudete potřebovat původní domény se systémem Windows NT, záložní řadiče domény se systémem Windows NT nebo doménu se systémem Windows 2000.

Režim Windows Server 2008

Po provedení upgradu systémů Windows NT a Windows 2000 ve vaší organizaci můžete pokračovat upgradem na systémy Windows Server 2008. To provedete jako upgrade řadičů domény se systémem Windows 2003 na řadiče domény se systémem Windows Server 2008 nebo Windows Server 2008 a poté, pokud to bude zapotřebí, můžete změnit úroveň funkčnosti na podporu režimu Windows Server 2008.

Před aktualizací řadičů domény se systémem Windows Server 2003 byste měli nejprve připravit doménu na systém Windows Server 2008. K provedení aktualizace schémat doménové struktury a domény tak, aby byla kompatibilní s doménami se systémem Windows Server 2008, budete muset použít nástroj Adprep.exe:

1. Na hlavním operačním serveru schématu doménové struktury zkopírujte obsah složky Sources\Adprep z instalačního média se systémem Windows Server 2008 do místní složky a poté spusťte příkaz **adprep/forestprep**. Pokud hodláte instalovat libovolné řadiče domény jen pro čtení, měli byste rovněž spustit příkaz **adprep/ /rodcprep**. Budete muset použít účet správce, který je členem skupiny Enterprise Admins, Schema Admins nebo Domain Admins v kořenové doméně doménové struktury.
2. Na hlavním operačním serveru infrastruktury pro každou doménu v doménové struktuře zkopírujte obsah složky Sources\Adprep z instalačního média se systémem Windows Server 2008 do místní složky a poté spusťte příkaz **adprep/domainprep/gpprep**. Budete muset použít účet správce, který je členem skupiny Domain Admins v příslušné doméně.

Jako vždy byste měli tyto postupy nejprve ověřit v laboratorním prostředí.

Poznámka: Abyste určili, který server je aktuálním hlavním operačním serverem schématu domény, zadejte v příkazovém řádku příkaz dsquery server -hasfsmo schema. Abyste určili, který server v doméně je hlavním operačním serverem infrastruktury dané domény, zadejte na příkazovém řádku příkaz dsquery server -hasfsmo infr.

Po provedení upgradu všech řadičů domény na systém Windows Server 2008 můžete zvýšit úroveň funkčnosti domény a doménové struktury, abyste mohli využívat nejnovější funkce služby Active Directory. Pokud to provedete, budete moci v doméně používat pouze prostředky systému Windows Server 2008 a nebudete se moci vrátit k žádnému předchozímu režimu. Proto byste měli režim Windows Server 2008 použít pouze

tehdy, pokud si budete jisti, že již nebudete potřebovat původní domény se systémem Windows NT, záložní řadiče domény se systémem Windows NT nebo doménu se systémem Windows 2000 nebo Windows Server 2003.

Zvýšení funkčnosti domény a doménové struktury

Domény s úrovní funkčnosti Windows Server 2003 nebo vyšší úrovní funkčnosti mohou využívat mnohé nové funkce domény Active Directory včetně univerzálních skupin, vnořování skupin, převodů typů skupin, aktualizace časových razítek přihlášení a verze klíčů služby distribuce klíčů modulu Kerberos (KDC). V tomto režimu mohou správci:

- Přejmenovat řadiče domény bez předchozího odinstalování role řadiče.
- Přejmenovat domény s řadiči domény se systémy Windows Server 2008.
- Vytvořit obousměrné vztahy důvěryhodnosti mezi dvěma doménovými strukturami.
- Provést restrukturalizaci domén jejich přejmenováním a přesunutím do jiné úrovně v hierarchii.
- Využívat možností replikací pro jednotlivé členy skupin a globální katalogy.

Doménové struktury domén s úrovní funkčnosti Windows Server 2003 nebo vyšší úrovní funkčnosti mohou využívat mnohé nové funkce služby Active Directory, kam patří vylepšená replikace globálního katalogu a efektivní replikace v rámci sítí i mezi nimi, a také schopnost konfigurovat jednosměrné, obousměrné a přenosné vztahy důvěryhodnosti mezi doménovými strukturami.

Z praxe: Proces upgradu domén a doménové struktury může v síti vyvolat značné replikace. V některých případech může trvat dokončení celého procesu upgradu 15 minut nebo déle. Během této doby se mohou při komunikaci se servery projevit delší odezvy a delší reakční doba v síti. Proto může být vhodné naplánovat upgrade mimo běžnou pracovní dobu. Je také vhodné důkladně ověřit kompatibilitu s existujícími aplikacemi (týká se především starších aplikací).

Úroveň funkčnosti domény můžete zvýšit podle následujících pokynů:

1. Klepněte na tlačítko Start, přejděte na položku Nástroje pro správu (Administrative Tools) a klepněte na položku Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts).
2. Pravým tlačítkem myši klepněte ve stromu konzoly na doménu, se kterou chcete pracovat, a v místní nabídce poté klepněte na příkaz Zvýšit úroveň funkčnosti domény (Raise Domain Functional Level).
3. Aktuální název domény a úroveň funkčnosti jsou zobrazeny v dialogovém okně Zvýšit úroveň funkčnosti domény (Raise Domain Functional Level).

4. Pokud chcete změnit úroveň funkčnosti domény, vyberte v seznamu novou úroveň funkčnosti a poté klepněte na příkaz Zvýšit (Raise). Tuto akci však bohužel nemůžete vrátit. Předtím, než ji provedete, pečlivě zvažte možné důsledky.
5. Po klepnutí na tlačítko OK se bude nová úroveň funkčnosti domény replikovat na všechny řadiče domény. Provedení této operace může ve velké organizaci nějakou dobu trvat.

Úroveň funkčnosti doménové struktury můžete zvýšit podle následujících pokynů:

1. Klepněte na tlačítko Start, přejděte na položku Nástroje pro správu (Administrative Tools) a klepněte na položku Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts).
2. Pravým tlačítkem myši klepněte ve stromu konzoly na doménu, se kterou chcete pracovat, a v místní nabídce poté klepněte na příkaz Zvýšit úroveň funkčnosti doménové struktury (Raise Forest Functional Level).
3. Aktuální název doménové struktury a úroveň funkčnosti jsou zobrazeny v dialogovém okně Zvýšit úroveň funkčnosti doménové struktury (Raise Forest Functional Level).
4. Pokud chcete změnit úroveň funkčnosti doménové struktury, vyberte v seznamu novou úroveň funkčnosti a poté klepněte na příkaz Zvýšit (Raise). Tuto akci však bohužel nemůžete vrátit. Předtím, než ji provedete, pečlivě zvažte možné důsledky.
5. Po klepnutí na tlačítko OK se bude nová úroveň funkčnosti domény replikovat na všechny řadiče domény ve všech doménách doménové struktury. Provedení této operace může ve velké organizaci nějakou dobu trvat.

Základy struktury adresářové služby

Služba Active Directory má mnoho součástí a je založena na mnoha technologiích. Její data jsou zpřístupněna uživatelům a počítačům prostřednictvím úložišť dat a globálních katalogů. Přestože většina úkolů služby Active Directory ovlivňuje úložiště dat, jsou globální katalogy stejně důležité, neboť se využívají při přihlašování a při hledání informací. Pokud není globální katalog k dispozici, nemohou se běžní doménoví uživatelé přihlásit. Jediným způsobem, jak toto chování změnit, je ukládat členství v univerzálních skupinách do místní mezipaměti. Toto řešení má své výhody i nevýhody, které jsou popsány dále.

K datům služby Active Directory se přistupuje pomocí protokolů pro přístup k adresářové službě a její data se distribuují pomocí replikací. Protokoly pro přístup k adresářové službě umožňují klientským počítačům komunikovat s řadiči domény. Replikace zajišťuje distribuci aktualizovaných dat na řadiče domény. Přestože je replikace adresářových informací vždy typu multimaster, některé změny dat mohou provádět pouze individuální řadiče domény nazývané *hlavní operační servery* (operations master). Na

replikace typu multimaster má také vliv nová vlastnost systému Windows Server 2008 nazvaná *oddíl adresáře aplikace* (application directory partition).

Správci velkých sítí (členové skupiny Enterprise Admins) mohou v doménové struktuře vytvářet oddíly adresáře aplikací. Jedná se o logické struktury, pomocí kterých se řídí replikace dat v doménové struktuře. Je například možné vytvořit oddíl, který bude přesně určovat replikaci dat služby DNS v doméně. Ostatním systémům v doméně se tak zabrání v její replikaci.

Oddíl adresáře aplikací se může objevit jako podřízený objekt domény, podřízený objekt jiného oddílu adresáře aplikací nebo jako nový strom ve stávající doménové struktuře. Jeho replika může být zpřístupněna na jakémkoli řadiči domény Active Directory se systémem Windows Server 2008, včetně globálních katalogů. Přestože jsou oddíly adresáře aplikací ve velkých doménách a doménových strukturách užitečné, jsou přítěží při plánování, správě a údržbě.

Úložiště dat

Úložiště dat obsahuje informace o objektech, jako jsou účty, sdílené prostředky, organizační jednotky a zásady skupiny. Jiným názvem pro úložiště dat je *adresář*, což se týká přímo služby Active Directory.

Řadiče domény ukládají adresář v souboru Ntds.dit. Umístění tohoto souboru se určuje během instalace domény Active Directory a musí být na jednotce zformátované systémem souborů NTFS, aby s ní dokázal systém Windows Server 2008 pracovat. Adresářová data je také možné uložit odděleně od hlavního úložiště dat. To platí pro zásady skupiny, skripty a další typy veřejných informací, které jsou uložené ve sdílené systémové složce (Sysvol).

Protože je úložiště dat kontejnerem pro objekty, sdílení adresářových informací se nazývá *zveřejnění*. Informace o tiskárně se například zveřejní při jejím sdílení v síti. Podobným způsobem zveřejníte informace o složce jejím sdílením v síti.

Většinu změn replikují řadiče domény pomocí replikace typu multimaster. Jako správci středně velké organizace budete jen zřídka potřebovat tyto replikace spravovat. Replikace se provádí automaticky, ale můžete je upravit tak, aby vyhovovaly potřebám velkých organizací nebo organizací se speciálními požadavky.

Ne všechna adresářová data se replikují. Replikují se veřejné informace spadající do jedné z následujících tří kategorií:

- **Doménová data** – obsahují informace o objektech v rámci domény. Patří sem objekty pro účty, sdílené prostředky, organizační jednotky a zásady skupiny.
- **Konfigurační data** – popisují topologii adresářové služby. Zahrnují seznam všech domén, stromů a doménových struktur a také umístění řadičů domény a serverů globálního katalogu.

- **Data schématu** – popisují všechny objekty a typy dat, které mohou být v adresářové službě uloženy. Výchozí schéma systému Windows Server 2008 popisuje objekty účtů, objekty sdílených prostředků a další. Výchozí schéma můžete rozšířit definováním nových objektů a atributů nebo přidáním atributů do existujících objektů.

Globální katalogy

Pokud se členství v univerzálních skupinách neukládá do místní mezipaměti, jsou globální katalogy (Global Catalogs) nutné pro přihlášení k síti, neboť při zahájení přihlašovacího procesu poskytují informace o členství v univerzálních skupinách. Globální katalogy také umožňují hledání ve všech doménách doménové struktury. Řadič domény plnící zároveň roli globálního katalogu uchovává úplnou repliku všech objektů adresářové služby z vlastní domény a částečnou repliku všech ostatních domén doménové struktury.

Poznámka: Protože jsou pro přihlášení a při hledání podstatné pouze některé atributy, udržuje se na globálních katalozích pouze část atributů objektů ostatních domén doménové struktury. Částečná replikace také znamená, že se v síti přenáší méně informací a omezuje se tak provoz v síti.

Globálním katalogem je standardně první nainstalovaný řadič domény. Pokud v doméně existuje jediný řadič domény, je role řadiče domény a globální katalog na stejném serveru. Jinak je globální katalog na tom řadiči domény, kde jsme jej nakonfigurovali. Do domény můžete přidat další globální katalogy, abyste napomohli zlepšení odezvy při přihlašování a při hledání. V každé síti by měl být jeden řadič domény.

Řadiče domény, které jsou hostitelem globálního katalogu, by měly být pomocí rychlého spojení připojené k řadičům domény plnícím roli hlavních serverů infrastruktury. Role hlavního serveru infrastruktury je jednou z pěti rolí hlavních operačních serverů, kterou můžete přiřadit řadiči domény. V doméně odpovídá za aktualizování odkazů na objekty. Provádí to porovnáváním svých dat s daty globálního katalogu. Pokud nalezne zastaralá data, vyžádá si z globálního katalogu aktuální data. Poté provede replikaci změn do ostatních řadičů domény v doméně. Další informace o rolích hlavních operačních serverů naleznete dále v této kapitole v části „Role hlavních operačních serverů".

Pokud je v doméně pouze jeden řadič domény, můžete přidělit roli hlavního serveru infrastruktury a globální katalog stejnému řadiči. Pokud v doméně existují dva nebo více řadičů, musí být globální katalog a hlavní server infrastruktury na oddělených řadičích domény. Pokud nejsou, nenalezne hlavní server infrastruktury zastaralá data, a proto nebude nikdy replikovat změny. Jedinou výjimkou je, když všechny řadiče v doméně hostují globální katalog. V tomto případě nezáleží na tom, který řadič domény plní roli hlavního serveru infrastruktury.

Jedním z hlavních důvodů, proč v doméně konfigurovat další globální katalog, je zajištění dostupnosti globálního katalogu při přihlašování a při požadavcích na hledání v adresářové službě. Pokud má doména pouze jediný globální katalog, ten není k dis-

pozici a není nakonfigurováno ukládání členství v univerzálních skupinách do místní mezipaměti, nemohou se běžní uživatelé přihlásit a nelze hledat v adresářové službě. Jedinými uživateli, kteří se v takovém případě přihlásí, jsou členové skupiny Domain Admins.

Hledání v globálním katalogu je velmi efektivní. Katalog obsahuje informace o objektech ze všech domén doménové struktury. Tím je umožněno, aby požadavky hledání v adresářové službě byly vyřešeny v místní doméně, než v doméně v jiné části sítě. Místní řešení dotazů snižuje zatížení sítě a ve většině případů umožňuje rychlejší odpovědi.

Tip: Pokud jste si všimli pomalého přihlašování nebo delších časů odpovědí na dotazy, může být řešením konfigurace dalších globálních katalogů. Více globálních katalogů však obvykle znamená více replikačních dat, která se v síti přenášejí.

Ukládání členství v univerzálních skupinách do mezipaměti

Ve velké organizaci nemusí být praktické mít globální katalogy v každé pobočce. Pokud nebudou v každé pobočce globální katalogy, může to být problém. Pokud nebude mít pobočka spojení s centrálou nebo jinou pobočkou, kde severy globálního katalogu jsou, nebudou se moci přihlásit běžní uživatelé, ale pouze členové skupiny Domain Admins. To proto, že požadavky na přihlášení musí být směrovány po síti na server globálního katalogu v jiné pobočce, a kvůli neexistenci spojení to není možné.

Existuje více způsobů, jak se tomuto stavu vyhnout. Podle postupu uvedeného v části „Konfigurace globálních katalogů" v kapitole 8, „Základy správy služby Active Directory" můžete některým řadičům domény udělit roli globálního katalogu. Nevýhodou je jejich vyšší zatížení, které může vyžadovat další systémové prostředky. Dále je nutné pečlivě řídit dostupnost serverů globálního katalogu.

Dalším způsobem je ukládat místně informace o členství v univerzálních skupinách. Požadavek na přihlášení tak může vyřešit jakýkoli řadič domény bez nutnosti kontaktovat server globálního katalogu. Rychlost přihlášení je vyšší a zároveň je jednodušší správa výpadků serverů: doména není při přihlašování závislá na jednom serveru nebo skupině serverů. Toto řešení rovněž snižuje zatížení sítě způsobené replikacemi. Místo pravidelné replikace celého globálního katalogu přes síť se obnovují pouze informace o členství v univerzálních skupinách v mezipaměti. Obnovení probíhá standardně každých osm hodin.

Členství v univerzálních skupinách je závislé na sítích. Síť je fyzickou strukturou adresářové služby sestávající z jedné nebo více podsítí se specifickým rozsahem adres IP a maskou podsítě. Řadiče domény se systémem Windows Server 2008 a globální katalog, který kontaktují, musí být ve stejné síti. Pokud máte více sítí, budete muset nakonfigurovat ukládání do mezipaměti v každé z nich. Uživatelé musí být navíc součástí

domény se systémem Windows Server 2008 s úrovní funkčnosti doménové struktury Windows Server 2008. Další informace o konfiguraci ukládání do mezipaměti naleznete v kapitole 8 v části „Konfigurace ukládání členství v univerzálních skupinách do mezipaměti".

Replikace a služba Active Directory

Bez ohledu na to, zda používáte replikaci FRS nebo DFS, třemi typy informací, které jsou součástí adresářové služby, jsou doménová data, data schématu a konfigurační data.

Data domény se v rámci domény replikují na všechny řadiče domény. Data schématu a konfigurační data se replikují do všech domén stromu nebo doménové struktury. Všechny objekty v dané doméně a některé z vlastností všech ostatních objektů doménové struktury se replikují do globálních katalogů.

Znamená to, že doménové řadiče ukládají a replikují následující položky:

- informace o schématu pro celý strom či doménovou strukturu;
- konfigurační informace pro všechny domény stromu či doménové struktury;
- všechny adresářové objekty a vlastnosti svých domén.

Řadiče domény hostující globální katalog ukládají a replikují informace schématu celé doménové struktury, konfigurační informace všech domén doménové struktury, podmnožinu vlastností všech adresářových objektů celé doménové struktury, které se replikují pouze mezi servery globálního katalogu a všechny adresářové objekty své domény.

Následující scénář instalace nové sítě slouží k lepšímu pochopení replikací.

1. V doméně A nainstalujete první řadič domény. Bude se jednat o jediný řadič domény, který bude zároveň hostovat globální katalog. Protože nejsou v síti další řadiče, nebude docházet k replikacím.

2. Do domény A nainstalujete druhý řadič domény. Protože nyní existují dva řadiče, začne probíhat replikace. Pro zajištění správné replikace dat přiřaďte jednomu ze serverů roli hlavního serveru infrastruktury a druhému roli globálního katalogu. Hlavní server infrastruktury sleduje aktualizace globálního katalogu a žádá o aktualizaci změněných objektů. Dva řadiče domény dále replikují schéma a konfigurační data.

3. Do domény A nainstalujete třetí řadič domény. Ten není globálním katalogem. Hlavní server infrastruktury sleduje aktualizace globálního katalogu, žádá o aktualizaci změněných objektů a replikuje je na třetí řadič domény. Tři řadiče domény dále replikují schéma a konfigurační data.

4. Nainstalujete novou doménu B a přidáte do ní řadiče domény. Servery globálního katalogu v doméně A a B začnou replikovat schéma a konfigurační data a pod-

množinu doménových dat každé domény. Replikace v doméně A pokračuje tak, jak bylo popsáno výše. Replikace v doméně B začíná.

Služba Active Directory a protokol LDAP

Protokol LDAP (Lightweight Directory Access Protocol) je standardním internetovým komunikačním protokolem v sítích TCP/IP. Je konkrétně navržen pro přístup k adresářové službě s co nejmenším zatížením. Dále určuje operace, které se mohou využívat v dotazech a při úpravách adresářových informací.

Služba Active Directory používá protokol LDAP při komunikaci s řadiči domény při každém přihlášení a při hledání prostředků v síti. Dále se využívá při správě domény Active Directory.

Protokol LDAP je otevřeným standardem, který mohou využívat další adresářové služby. Komunikace mezi adresářovými službami je tak jednodušší a jednodušší je i případná migrace jiných adresářových služeb do služby Active Directory. Pro rozšíření možností spolupráce lze využít také rozhraní pro přístup k Active Directory (Active Directory Service Interface, ADSI). ADSI využívá rozhraní pro programování aplikací (API) pro protokol LDAP specifikované v dokumentu RFC 1823. Rozhraní ADSI lze využívat i ve skriptech.

Role hlavních operačních serverů

Role operačních serverů zajišťují úlohy, které nelze provádět na více místech. Existuje pět rolí operačních serverů, které lze přiřadit jednomu nebo více řadičům domény. Ačkoli lze některé z nich přiřadit v doménové struktuře pouze jednou, ostatní musí být definovány v každé doméně.

Každá služba Active Directory musí mít následující role:

- **Hlavní server schémat (Schema master)** – řídí aktualizace a úpravy schématu adresářové služby. Pokud chcete schéma upravit, musíte mít přístup k hlavnímu serveru schémat. Abyste zjistili, který server je momentálně hlavním serverem schémat, spusťte příkazový řádek a zadejte v něm příkaz **dsquery server –hasfsmo schema**.
- **Hlavní názvový server domény (Domain naming master)** – řídí přidávání nebo odebírání domén v doménové struktuře. Pokud chcete přidat nebo odebrat doménu, musíte mít přístup k hlavnímu názvovému serveru domény. Abyste zjistili, který server je aktuálním hlavním názvovým serverem domény, spusťte příkazový řádek a zadejte v něm příkaz **dsquery server –hasfsmo name**.

Uvedené role na úrovni doménové struktury musí být v doménové struktuře jedinečné. To znamená, že v jedné doménové struktuře může existovat pouze jeden hlavní operační server schémat a jeden hlavní názvový server domény.

V každé doméně musí být následující role:

- **Hlavní server RID (Relative ID master)** – řadičům domény přiděluje relativní identifikátory ID. Při vytváření objektu uživatele, skupiny nebo počítače přiřadí řadič domény objektu identifikátor zabezpečení. Ten sestává z identifikátoru zabezpečení domény a z jedinečného relativního identifikátoru ID, který byl přidělen serverem RID. Abyste zjistili, který server je momentálně hlavním serverem RID, spusťte příkazový řádek a zadejte v něm příkaz **dsquery server –hasfsmo rid**.
- **Emulátor primárního řadiče domény (PDC emulator)** – ve smíšeném nebo provizorním režimu pracuje emulátor primárního řadiče domény jako primární řadič domény se systémem Windows NT. Jeho úkolem je ověřovat přihlášení systémů Windows NT, zpracovávat změny hesel a replikovat aktualizace na záložní řadiče domény. Abyste zjistili, který server je momentálně emulátorem primárního řadiče domény, spusťte příkazový řádek a zadejte v něm příkaz **dsquery server –hasfsmo pdc**.
- **Hlavní server infrastruktury (Infrastructure master)** – aktualizuje odkazy na objekty porovnáním svých adresářových dat s daty globálního katalogu. Pokud nejsou aktuální, vyžádá si od globálního katalogu aktualizace a poté je replikuje na ostatní řadiče domény v doméně. Abyste zjistili, který server je momentálně hlavním serverem infrastruktury, spusťte příkazový řádek a zadejte v něm příkaz **dsquery server –hasfsmo infr**.

Uvedené doménové role musí být v doméně jedinečné. To znamená, v každé doméně může být pouze jediný hlavní server RID, jeden emulátor primárního řadiče domény a jeden hlavní server infrastruktury.

Ve většině případů se role hlavních operačních serverů přiřadí automaticky, ale je možné jejich přiřazení změnit. Při instalaci sítě je první nainstalovaný řadič domény v první doméně držitelem všech rolí hlavních operačních serverů. Pokud později vytvoříte novou podřízenou doménu nebo kořenovou doménu nového stromu, bude první řadič domény automaticky držitelem doménových rolí operačních serverů. V nové doménové struktuře bude mít první řadič domény všech pět rolí operačních serverů. Pokud je nová doména součástí existující doménové struktury, bude mít řadič domény role hlavního serveru RID, emulátoru primárního řadiče domény a hlavního serveru infrastruktury. Hlavní server schémat a hlavní server pro pojmenování domén zůstávají v první doméně doménové struktury.

Pokud má doména jediný řadič domény, plní tento počítač role všech operačních serverů. Pokud pracujete s jedinou sítí, výchozí umístění hlavního operačního serveru by mělo být dostačující. Ovšem pokud přidáte řadiče domény a domény, nejspíše budete chtít role hlavního operačního serveru přesunout na jiné řadiče domény.

Pokud má doména dva a více řadičů domény, měli byste role operačních serverů svěřit alespoň dvěma řadičům.V takovém případě by jeden řadič domény sloužil jako hlavní operační server a druhý jako záložní operační server. Záložní operační server

se tedy používá v případě selhání hlavního operačního serveru. Přesvědčte se, že řadiče domény jsou přímými partnery replikace a jsou správně připojeny.

Ve větších doménách je vhodné role hlavních operačních serverů oddělit a přiřadit je odděleným řadičům domény, abyste zrychlili odezvy hlavních operačních serverů. Při přidělování rolí dbejte na aktuální stav řadičů domény a jejich odpovědnost.

Doporučený postup: Dvě role, které byste neměli oddělovat, jsou hlavní server schématu a hlavní server pro pojmenování domén. Tyto role vždy přiřaďte jednomu serveru. Z hlediska optimalizace operací by měly být na jednom řadiči domény společně také hlavní server RID a emulátor primárního řadiče domény. Pokud je to však nutné, můžete tyto role oddělit. K tomu může dojít například ve velkých sítích, které bývají ve špičkách velmi vytížené; v takových případech byste nejspíše chtěli umístit hlavní server RID a emulátor primárního řadiče domény na samostatné řadiče domény. Hlavní server infrastruktury by dále neměl být na řadiči domény hostujícím globální katalog. Další informace naleznete v části „Globální katalogy“ v této kapitole.