KAPITOLA 6

Konfigurace, údržba a řešení problémů s hlavními operačními servery

V této kapitole:

Model replikace multimaster služby Active Directory tvoří distribuované prostředí, které řadiči domény umožňuje jeho použití pro ověřování a vám umožňuje provádět změny standardních informací o adresáři bez ohledu na to, který řadič domény použijete. Tento přístup funguje bez problému pro většinu operací služby Active Directory – ovšem ne pro všechny.

Některé operace služby Active Directory je třeba pečlivě kontrolovat, aby byla dodržena integrita struktury adresáře a dat. Tyto operace může provádět pouze jediný autoritativní řadič domény označovaný jako hlavní operační server. Například změny schématu můžete provádět pouze na řadiči domény, který slouží jako hlavní server schémat; je-li tento server nedostupný, žádné změny schématu nelze provádět.

Jako správce máte zodpovědnost za zajištění nepřetržité dostupnosti a odpovídající konfigurace hlavních operačních serverů, aby byly schopny zpracovat své úlohy. V této kapitole se dozvíte o tom, jak se hlavní operační servery používají, stejně jako další informace o správě, údržbě a řešení problémů s hlavními operačními servery.

Základní informace o hlavním operačním serveru

Hlavní operační servery zajišťují správnou funkčnost adresáře prováděním specifických úloh, které nemohou provádět žádné jiné řadiče domény. Určený hlavní operační server plní roli FSMO (flexible single-master operations).

Představení hlavních operačních serverů

Jak můžete vidět v tabulce 6.1, existuje pět stanovených rolí hlavního operačního serveru, které lze uspořádat do dvou větších kategorií. Role na úrovni doménové struktury jsou přiřazeny pro jednotlivé doménové struktury. To znamená, že v doménové struktuře služby Active Directory existuje pouze jeden hlavní server schémat a pouze jeden hlavní server názvů domén. Role na úrovni domény jsou přiřazeny pro jednotlivé domény. To znamená, že pro každou doménu v doménové struktuře služby Active Directory existuje pouze jeden hlavní server infrastruktury, emulátor primárního řadiče domény a hlavní server RID.

Tabulka 6.1: Dostupné hlavní operační servery podle kategorie

Kategorie	Hlavní operační server
Na úrovni doménové struktury	Hlavní server názvů domén
	Hlavní server schémat
Na úrovni domény	Hlavní server infrastruktury
	Emulátor primárního řadiče domény (PDC)
	Hlavní server RID

V doménové struktuře služby Active Directory provádí hlavní server názvů domén a hlavní server schémat operace na úrovni doménové struktury. Hlavní server názvů domén řídí vytváření a odstraňování domén, přičemž garantuje, že každá doména je v rámci doménové struktury jedinečná. Hlavní server schémat spravuje schéma a vynucuje konzistenci schématu v celém adresáři.

V doméně služby Active Directory provádí hlavní server infrastruktury, emulátor primárního řadiče domény a hlavní server RID operace na úrovni domény. Hlavní server infrastruktury zpracovává mapování typu uživatel-skupina, změny členství ve skupinách a replikaci těchto změn na jiné řadiče domény. Emulátor primárního řadiče domény je zodpovědný za zpracování a replikaci změn hesel, a rovněž musí být dostupný pro resetování a ověření externích vztahů důvěryhodnosti. Hlavní server RID spravuje fond relativních identifikátorů (RID). Relativní identifikátory jsou číselné řetězce používané k vytvoření identifikátorů zabezpečení (SID) pro objekty zabezpečení.

První řadič domény, který nainstalujete v doménové struktuře, automaticky přijme roli hlavního serveru schémat a hlavního serveru názvů domén. Rovněž se stane hostitelem globálního katalogu. Jelikož tyto role jsou kompatibilní s globálním katalogem a přesunutí těchto rolí na jiné řadiče domény nevede ke zvýšení výkonu, můžete ponechat role na počátečním řadiči domény. Rovněž si uvědomte, že oddělení rolí vede k dalším administrativním režiím, neboť budete muset zjišťovat hlavní operační servery a implementovat procedury pro zálohování a obnovení.

Při instalaci prvního řadiče domény v nové doméně jsou mu přiřazeny tři role na úrovni domény. Obvykle budete chtít nechat tyto role na úrovni domény pohromadě, pokud vytížení vašeho hlavního operačního serveru nebude představovat pádný argu-

ment pro další zvýšení správy, které by s sebou oddělení rolí přineslo. Z tohoto důvodu budete pravděpodobně chtít v kořenových doménách, které nejsou kořenovými doménami doménové struktury, ponechat role na úrovni domény na prvním řadiči domény (pokud nekonfigurujete řadič domény jako server globálního katalogu).

Ovšem v případě kořenové domény doménové struktury je první řadič domény, vytvořený v dané doméně, hostitelem rolí na úrovni doménové struktury a všech tří rolí na úrovni domény, stejně jako hostitelem globálního katalogu. Ovšem role hlavního serveru infrastruktury není kompatibilní s globálním katalogem. Proto pokud instalujete druhý řadič domény v kořenové doméně doménové struktury, Průvodce instalací služby Active Directory Domain Services (Active Directory Domain Services Installation Wizard) vás vyzve k tomu, abyste mu povolili přenést roli hlavního serveru infrastruktury. Pokud tuto roli přenesete, možná budete po instalaci služby AD DS (Active Directory Domain Services) zvažovat také přenos rolí emulátoru primárního řadiče domény a hlavního serveru RID na druhý řadič domény. Tímto krokem docílíte ponechání zmíněných tří rolí na úrovni domény pohromadě, což usnadní správu.

Určení hlavních operačních serverů

Určit aktuální hlavní operační servery pro vaši přihlašovací doménu můžete zadáním následujícího příkazu v příkazovém řádku.

```
netdom query fsmo
```

Následující příklad vypisuje vlastníky jednotlivých rolí podle jejich plně kvalifikovaných názvů domény.

```
Hlavní server schémat              CentralDC17.cpandl.com
Hlav. názvový server domény        CentralDC17.cpandl.com
Primární řadič domény          CorpServer38.ny.cpandl.com
Správce fondu RID               CorpServer38.ny.cpandl.com
Hlav. server infrastruktury    CorpServer15.ny.cpandl.com
```

Z výše uvedeného výpisu můžete rovněž zjistit, že kořenovou doménou doménové struktury je cpandl.com a že aktuální přihlašovací doménou je ny.cpandl.com. Pokud chcete zjistit hlavní operační servery pro konkrétní doménu, použijte následující příkaz.

```
netdom query fsmo /d:Název_domény
```

Zde představuje *Název_domény* název dané domény, např. sales.cpandl.com.

Plánování pro hlavní operační servery

K provádění příslušných operací řadičů domény, které jsou hostiteli rolí hlavního operačního serveru, musí být nepřetržitě dostupné a musí být umístěny v oblastech vaší sítě s vysokou dostupností. V případě rozšíření vaší infrastruktury služby Active Directory přidáním domén a lokalit, bude hrát stále důležitější roli pečlivé umístění vašich hlavních operačních serverů.

Nesprávné umístění serverů plnících roli hlavního operačního serveru může:

- Znemožnit uživatelům a počítačům údržbu jejich hesel.
- Znemožnit správcům přidat domény a nové objekty.
- Znemožnit správcům provádět změny schématu.
- Znemožnit replikaci aktualizovaných informací o členství ve skupinách.

Se změnou vaší infrastruktury služby Active Directory musíte zabránit problémům spojeným s nesprávným umístěním role hlavního operačního serveru a možná budete muset znovu přiřadit role jiným řadičům domény. Při návrhu každé doménové struktury nebo domény zvažte počet řadičů domény, které budete potřebovat na jednu doménu, a také to, zdali budete muset po instalaci nových řadičů domény měnit hlavní operační servery.

Změna hlavních operačních serverů

Role hlavních operačních serverů lze změnit několika způsoby. Pokud je aktuální hlavní operační server v režimu online, můžete provést přenos role, a elegantně tak postoupit danou roli z jednoho řadiče domény na jiný. Pokud došlo k selhání aktuálního hlavního operačního serveru, a tento nepřejde zpět do režimu online, můžete danou roli převzít a vynutit její přenos na jiný řadič domény.

Pokud přenesete roli způsobem popsaným dále v této kapitole v části „Práce s hlavními operačními servery“, přesunete tím roli hlavního operačního serveru z jednoho řadiče domény na jiný. Během přenosu role si tyto dva řadiče domény vymění veškeré nereplikované informace, aby bylo zajištěno, že nedojde ke ztrátě žádných transakcí. Pokud tyto dva řadiče domény nejsou přímými partnery replikace, je možné, že před úplnou vzájemnou synchronizací obou řadičů domény bude potřeba replikovat značný objem informací. Pokud jsou tyto dva řadiče domény přímými partnery replikace, neprovedených transakcí by mělo být méně a operace přenesení role by měla proběhnout rychleji. Po dokončení přenosu se dřívější server plnící přenášenou roli už nadále nebude pokoušet plnit roli hlavního operačního serveru, a tím eliminuje možnost duplikace hlavních operačních serverů existujících v síti.

Přenos určité role je upřednostňován před převzetím dané role. Opětovné přiřazení dané role hlavního operačního serveru prostřednictvím jejího převzetí by mělo být až krajním řešením. Pokud musíte roli převzít, nikdy znovu nepřidávejte předchozího vlastníka role do sítě bez potřebných opatření, abyste zabránili předchozímu vlastníkovi dané role stát se znovu aktivním. V opačném případě může vést nekorektní přidání předchozího vlastníka role do sítě k neplatným datům a poškození dat v adresáři. Další informace najdete v části „Převzetí rolí hlavního operačního serveru“ dále v této kapitole.

Důvody k přenosu rolí hlavního operačního serveru závisí na mnoha faktorech. Za prvé, roli hlavního operačního serveru byste mohli chtít přenést za účelem zvýšení výkonu, což byste mohli učinit v případě přílišné vytíženosti serveru, kterou byste potřebovali

rozložit. Za druhé, roli hlavního operačního serveru byste mohli chtít přenést v případě, že plánujete uvést server plnící danou roli do režimu offline kvůli údržbě, nebo v případě selhání serveru. Mějte na paměti, že ačkoliv role hlavního operačního serveru může být umístěna na téměř kterémkoliv řadiči domény s možností zápisu, role hlavního operačního serveru nemohou být umístěny na řadičích domény jen pro čtení.

Při určování umístění hlavních operačních serverů byste měli umístit role na úrovni doménové struktury, hlavní server schémat a hlavní server názvů domén na stejný řadič domény. S těmito rolemi je spojeno velmi málo režií, takže umístění na stejný server zvýší celkové režie jen nepatrně. Ovšem je důležité tento server dobře zabezpečit, protože se jedná o zásadní role v doménové struktuře. Navíc, server sloužící jako hlavní server názvů domén by měl být rovněž serverem globálního katalogu.

Role hlavního serveru RID a emulátoru primárního řadiče domény (PDC) byste měli umístit na stejný řadič domény. Důvodem je, že emulátor primárního řadiče domény používá více relativních identifikátorů, než většina jiných řadičů domény. Pokud se role hlavního serveru RID a emulátoru primárního řadiče domény nenachází na stejném řadiči domény, řadiče domény, na nichž jsou tyto role umístěny, by se měly nacházet ve stejné lokalitě služby Active Directory, a mezi těmito řadiči domény by mělo existovat spolehlivé spojení.

Hlavní server infrastruktury byste neměli umisťovat na řadič domény, který je rovněž serverem globálního katalogu. Důvod k tomu je poněkud složitější a je třeba zmínit se o některých důležitých výjimkách. Hlavní server infrastruktury je zodpovědný za aktualizaci členství ve skupinách mezi doménami a zjišťuje, zdali jsou jeho informace aktuální, nebo zastaralé, kontrolou globálního katalogu a případnou replikací změn na ostatní řadiče domény. Pokud se hlavní server infrastruktury a globální katalog nachází na stejném serveru, hlavní server infrastruktury neví, o tom, že došlo k nějakým změnám, a proto je nereplikuje.

Výjimkou je doménová struktura s jedinou doménou nebo doménová struktura s více doménami, v níž jsou všechny řadiče domény servery globálního katalogu. V případě doménové struktury s jedinou doménou neexistují žádné odkazy mezi skupinami, které by bylo třeba aktualizovat, takže nezáleží na tom, kde se nachází hlavní server infrastruktury. V případě doménové struktury s více doménami, v níž jsou všechny řadiče domény servery globálního katalogu, všechny řadiče domény už vědí o všech objektech v dané doménové struktuře, takže hlavní server infrastruktury opravdu nemusí provádět aktualizaci.

Neměňte konfiguraci globálního katalogu řadiče domény, o kterém předpokládáte, že bude plnit roli hlavního operačního serveru. Úprava konfigurace globálního katalogu může způsobit změny v adresáři, které se mohou projevit až za několik dní, a řadič domény by nemusel být během této doby dostupný.

Práce s hlavními operačními servery

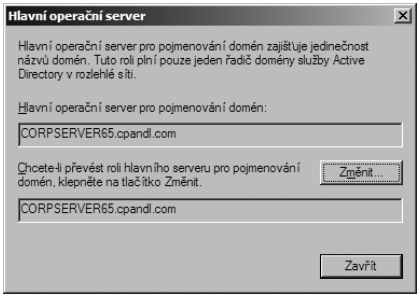
Klíčem k úspěšné správě hlavních operačních serverů je znalost, co každý hlavní operační server dělá, a být schopen rychle rozpoznat problémy, které nastanou, pokud hlavní operační server nefunguje správně. Kromě rad, které se týkaly umístění hlavních operačních serverů a o nichž jsem se zmínil již dříve, možná budete chtít zvážit přenos tří rolí na úrovni domény z prvního řadiče domény, který jste nainstalovali v kořenové doméně doménové struktury, na jiný, výkonnější řadič domény. Ve všech dalších doménách nechejte role na úrovni domény na prvním řadiči domény, pokud nemáte pádný důvod k přesunutí rolí. Nakonec byste měli připravit další řadiče domény jako záložní hlavní operační servery a měli byste pečlivě sledovat vytížení nejzatíženějšího hlavního operačního serveru – emulátoru primárního řadiče domény.

Správa hlavních serverů názvů domén

Hlavní server názvů domén je zodpovědný za přidání a odebrání domén z doménové struktury. Při každém vytvoření domény se vytvoří připojení vzdáleného volání procedury (RPC) k hlavnímu serveru názvů domén, který dané doméně přiřadí globálně jedinečný identifikátor (GUID). Kdykoliv při odebrání určité domény se vytvoří připojení RPC k hlavnímu serveru názvů domén a odstraní se odkaz na dříve přiřazený identifikátor GUID. Pokud se nemůžete připojit k hlavnímu serveru názvů domén, když se pokoušíte přidat nebo odebrat určitou doménu, doménu nebudete moci vytvořit nebo odebrat.

Hlavní server názvů domén můžete vyhledat pomocí následujících kroků:

1. Spusťte nástroj Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts) z nabídky Nástroje pro správu (Administrative Tools).
2. Klepněte pravým tlačítkem myši na uzlu Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts) a poté zvolte příkaz Hlavní operační server (Operations Master).
3. Dialogové okno Hlavní operační server (Operations Master), znázorněné na obrázku 6.1, zobrazí aktuální hlavní server názvů domén.



Obrázek 6.1: Vyhledejte hlavní server názvů domén

Roli hlavního serveru názvů domén můžete přenést na jiný server pomocí následujících kroků:

1. Spusťte nástroj Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts). Klepněte pravým tlačítkem myši na uzlu Domény

a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts) a poté zvolte příkaz Změnit řadič domény služby Active Directory (Change Active Directory Domain Controller).

2. V dialogovém okně Změnit adresářový server (Change Directory Server) zvolte možnost Tento řadič domény nebo instance služby AD LDS (This Domain Controller). Zadejte název kořenové domény doménové struktury do pole Vyhledat v této doméně (Look In This Domain) a poté stiskněte klávesu Tab.
3. Dostupné řadiče domény se zobrazí podle lokality, typu a verze operačního systému. Vyberte dostupný řadič domény, na který chcete přenést roli hlavního serveru názvů domén, a poté klepněte na tlačítko OK.
4. Klepněte pravým tlačítkem myši na uzel Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts) a poté klepněte na příkaz Hlavní operační server (Operations Master). Název aktuálního hlavního serveru názvů domén se objeví v prvním textovém poli. Řadič domény, na který chcete přenést roli hlavního serveru názvů domén, by se měl objevit ve druhém textovém poli. Pokud tomu tak není, zopakujte tuto proceduru počínaje krokem 1.
5. V dialogovém okně Hlavní operační server (Operations Master) klepněte na tlačítko Změnit (Change). Po vyzvání klepněte na tlačítko Ano (Yes) a potvrďte tak, že chcete přenést roli.
6. Po dokončení přenosu se zobrazí zpráva potvrzující přenos. Klepněte na tlačítko OK. Klepnutím na tlačítko Zavřít (Close) zavřete dialogové okno Hlavní operační server (Operations Master).

Správa hlavních serverů infrastruktury

Hlavní server infrastruktury je zodpovědný za aktualizaci objektů a hodnot všech atributů s rozlišujícími názvy, které se odkazují na objekty mimo aktuální doménu. Tyto aktualizace jsou obzvlášť důležité pro odkazování ze skupiny na objekty zabezpečení mezi doménami, kdy je hlavní server infrastruktury zodpovědný za to, že změny běžných názvů zaregistrovaných objektů zabezpečení se správně projeví v informacích o členství ve skupinách pro skupiny v ostatních doménách v doménové struktuře. Hlavní server infrastruktury tak učiní srovnáním svých dat adresáře s daty globálního katalogu. Pokud jsou data zastaralá, provede jejich aktualizaci a replikuje změny na ostatní řadiče domény v dané doméně. Pokud je z nějakého důvodu hlavní server infrastruktury nedostupný, odkazy mezi skupinou a objekty zabezpečení nebudou aktualizovány a členství ve skupinách mezi doménami nemusí přesně reflektovat skutečné názvy zaregistrovaných objektů zabezpečení.

Abyste pochopili, jak tento proces funguje, uveďme si následující příklad:

1. Uživatelka v doméně A je členem skupiny v doméně B. Uživatelka se provdá a její příjmení se v první doméně změní. Tato změna ovlivní atributy týkající se jména příslušného uživatelského objektu, včetně atributů Zobrazované jméno (Full Name)

a Příjmení (Last Name), a obvykle se změní také hodnota atributu DN daného uživatelského objektu. (Rozlišující název (DN) je hodnotou, která se použije v členském atributu objektů skupin.)

2. Jelikož řadiče domény v jedné doméně neprovádí replikaci objektů zabezpečení na řadiče domény v jiné doméně, druhá doména se o této změně nikdy nedozví. Následkem toho může zastaralá hodnota členského atributu skupiny v jiné doméně způsobit odepření oprávnění uživateli, jehož jméno se změnilo.
3. Aby byla zajištěna konzistence mezi doménami, hlavní server infrastruktury sleduje objekty zabezpečení z jiných domén. Pokud nalezne odkaz mezi doménami, porovná hodnotu jeho uloženého rozlišujícího názvu s hodnotou rozlišujícího názvu v původní doméně, aby zjistil, zda se informace změnila. Pokud se rozlišující název změnil, hlavní server infrastruktury provede aktualizaci a poté změnu replikuje na ostatní řadiče domény ve své doméně.

Tip: Kromě hlavního serveru infrastruktury můžete přiřadit role hlavního operačního serveru libovolnému řadiči domény bez ohledu na ostatní funkce adresáře, které daný řadič domény nabízí. Neumisťujte roli hlavního serveru infrastruktury na řadič domény, který rovněž slouží jako server globálního katalogu, pokud všechny řadiče domény v dané doméně nejsou servery globálního katalogu, nebo pokud doménové struktura neobsahuje pouze jednu doménu. Pokud je řadič domény, který je hostitelem role hlavního serveru infrastruktury, nakonfigurován jako server globálního katalogu, musíte přenést roli hlavního serveru infrastruktury na jiný řadič domény.

Z praxe: Hlavní server infrastruktury není kompatibilní s globálním katalogem a nesmí být umístěn na serveru globálního katalogu. Ovšem pokud jsou všechny řadiče domény v určité doméně servery globálního katalogu, řadič domény, který je hostitelem role hlavního serveru infrastruktury, je bezvýznamný, protože servery globálního katalogu replikují aktualizované informace o objektech zabezpečení na všechny ostatní servery globálního katalogu. Pokud doménová struktura obsahuje pouze jednu doménu, role hlavního serveru infrastruktury je rovněž bezvýznamná, protože objekty zabezpečení z jiných domén neexistují.

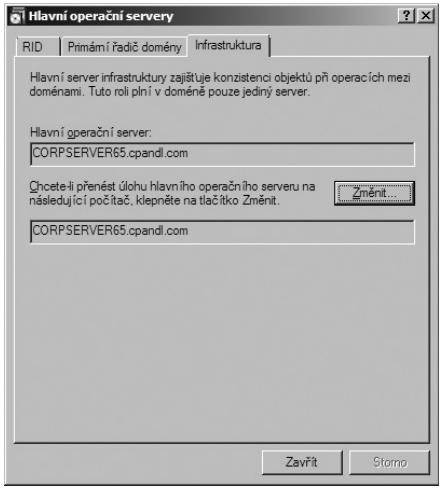
Hlavní server infrastruktury můžete vyhledat pomocí následujících kroků:

1. Spusťte nástroj Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) z nabídky Nástroje pro správu (Administrative Tools).
2. Pokud doména, se kterou chcete pracovat, není již zobrazena, klepněte pravým tlačítkem myši na uzel Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) a poté zvolte příkaz Změnit doménu (Change Domain). V dialogovém okně Změnit doménu (Change Domain) zadejte název DNS domény, se kterou chcete pracovat, například **cs.cpandl.com**, a poté klepněte na tlačítko OK.

3. Klepněte pravým tlačítkem myši na doméně, se kterou chcete pracovat, a poté zvolte příkaz Hlavní operační servery (Operations Masters).
4. V dialogovém okně Hlavní operační servery (Operations Masters) se zobrazí aktuální hlavní server infrastruktury na kartě Infrastruktura (Infrastructure). (Viz obrázek 6.2.)

Roli hlavního serveru infrastruktury můžete přenést na jiný server pomocí následujících kroků:

1. Spusťte nástroj Uživatelé a počítače služby Active Directory (Active Directory Users And Computers). Pokud doména, se kterou chcete pracovat, není již zobrazena, klepněte pravým tlačítkem myši na uzel Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) a poté zvolte příkaz Změnit doménu (Change Domain). V dialogovém okně Změnit doménu (Change Domain) zadejte název DNS domény, se kterou chcete pracovat, například **cs.cpandl.com**, a poté klepněte na tlačítko OK.
2. Klepněte pravým tlačítkem myši na uzlu domény a poté zvolte příkaz Změnit řadič domény (Change Domain Controller). V dialogovém okně Změnit adresářový server (Change Directory Server) zvolte možnost Tento řadič domény nebo instance služby AD LDS (This Domain Controller). Vyberte dostupný řadič domény, na který chcete přenést roli hlavního serveru infrastruktury, a poté klepněte na tlačítko OK.
3. Opět klepněte pravým tlačítkem myši na uzlu domény a poté zvolte příkaz Hlavní operační servery (Operations Masters). V dialogovém okně Hlavní operační servery (Operations Masters) vyberte kartu Infrastruktura (Infrastructure). Název aktuálního hlavního serveru infrastruktury se objeví v prvním textovém poli. Řadič domény, na který chcete přenést roli hlavního serveru infrastruktury, by se měl objevit ve druhém textovém poli. Pokud tomu tak není, zopakujte tuto proceduru počínaje krokem 1.
4. Klepněte na tlačítko Změnit (Change). Po vyzvání klepněte na tlačítko Ano (Yes) a potvrďte tak, že chcete přenést roli.
5. Po dokončení přenosu se zobrazí zpráva potvrzující přenos. Klepněte na tlačítko OK. Klepnutím na tlačítko Zavřít (Close) zavřete dialogové okno Hlavní operační servery (Operations Masters).



Obrázek 6.2: Vyhledejte hlavní server infrastruktury

Správa emulátorů primárního řadiče domény (PDC)

Když byla poprvé uvolněna služba Active Directory a doménové struktury služby Active Directory fungovaly ve smíšeném režimu Windows 2000, primární úlohou emulátoru primárního řadiče domény hlavního operačního serveru bylo zpracovat všechny požadavky na replikaci od záložních řadičů domény (BDC) se systémem Windows NT Server 4.0. V doméně používající úroveň funkčnosti Windows 2000 native nebo vyšší úroveň funkčnosti je řadič domény s rolí emulátoru primárního řadiče domény zodpovědný za zpracování změn hesel. Pokud uživatel změní heslo, tato změna je nejprve odeslána emulátoru primárního řadiče domény, který následně replikuje tuto změnu na všechny ostatní řadiče domény v dané doméně. To z emulátoru primárního řadiče domény činí rozhodující zdroj nejnovějších informací o heslech vždy, když dojde k selhání pokusu o přihlášení následkem zadání špatného hesla.

Každý řadič domény v doméně ví, který server plní roli emulátoru primárního řadiče domény. Pokud se uživatel pokusí přihlásit k síti, ale zadá nesprávné heslo, řadič domény prostřednictvím emulátoru primárního řadiče domény zjistí, zda obsahuje informaci o poslední změně hesla daného účtu. Pokud ano, řadič domény znovu zkusí ověřit přihlášení na emulátoru primárního řadiče domény. Tento postup je navržen tak, aby zajistil, že pokud si uživatel změnil heslo, není mu odepřeno přihlášení pomocí nového hesla.

Následkem této aktivity ověřující přihlášení je skutečnost, že role emulátoru primárního řadiče domény hlavního operačního serveru má ze všech rolí hlavního operačního serveru nejvyšší vliv na výkonnost řadiče domény, který je hostitelem této role. Uvědomte si, že pokud je v dané doméně nainstalován řadič domény jen pro čtení, role emulátoru primárního řadiče domény musí být umístěna na řadiči domény se systémem Windows Server 2008. A také si uvědomte, že emulátor primárního řadiče domény v kořenové doméně doménové struktury je rovněž výchozím zdrojem času služby Systémový čas (Windows Time) (W32time) pro doménovou strukturu.

Emulátor primárního řadiče domény můžete vyhledat pomocí následujících kroků:

1. Spusťte nástroj Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) z nabídky Nástroje pro správu (Administrative Tools). Pokud doména, se kterou chcete pracovat, není již zobrazena, klepněte pravým tlačítkem myši na uzlu Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) a poté zvolte příkaz Změnit doménu (Change Domain). V dialogovém okně Změnit doménu (Change Domain) zadejte název DNS domény, se kterou chcete pracovat, například **cs.cpandl.com**, a poté klepněte na tlačítko OK.
2. Klepněte pravým tlačítkem myši na uzlu domény a poté zvolte příkaz Hlavní operační servery (Operations Masters).
3. V dialogovém okně Hlavní operační servery (Operations Masters) se na kartě PDC zobrazí aktuální emulátor primárního řadiče domény. (Viz obrázek 6.3.)

Roli emulátoru primárního řadiče domény můžete přenést na jiný server pomocí následujících kroků:

1. Spusťte nástroj Uživatelé a počítače služby Active Directory (Active Directory Users And Computers). Pokud doména, se kterou chcete pracovat, není již zobrazena, klepněte pravým tlačítkem myši na uzlu Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) a poté zvolte příkaz Změnit doménu (Change Domain). V dialogovém okně Změnit doménu (Change Domain) zadejte název DNS domény, se kterou chcete pracovat, například **cs.cpandl.com**, a poté klepněte na tlačítko OK.

Obrázek 6.3: Vyhledejte emulátor primárního řadiče domény

2. Klepněte pravým tlačítkem myši na uzlu domény a poté zvolte příkaz Změnit řadič domény (Change Domain Controller). V dialogovém okně Změnit adresářový server (Change Directory Server) zvolte možnost Tento řadič domény nebo instance služby AD LDS (This Domain Controller). Vyberte dostupný řadič domény, na který chcete přenést roli emulátoru primárního řadiče domény, a poté klepněte na tlačítko OK.
3. Opět klepněte pravým tlačítkem myši na uzlu domény a poté zvolte příkaz Hlavní operační servery (Operations Masters). V dialogovém okně Hlavní operační servery (Operations Masters) vyberte kartu PDC. Název aktuálního emulátoru primárního řadiče domény se objeví v prvním textovém poli. Řadič domény, na který chcete přenést roli emulátoru primárního řadiče domény, by se měl objevit ve druhém textovém poli. Pokud tomu tak není, zopakujte tuto proceduru počínaje krokem 1.
4. Klepněte na tlačítko Změnit (Change). Po vyzvání klepněte na tlačítko Ano (Yes) a potvrďte tak, že chcete přenést roli.
5. Po dokončení přenosu se zobrazí zpráva potvrzující přenos. Klepněte na tlačítko OK. Klepnutím na tlačítko Zavřít (Close) zavřete dialogové okno Hlavní operační servery (Operations Masters).

Správa hlavních serverů RID

Hlavní server RID řídí vytváření nových objektů zabezpečení, jako jsou uživatelé, skupiny a počítače, v celé jeho související doméně. Pro každý řadič domény v dané doméně vydá hlavní server RID blok relativních identifikátorů. Tyto relativní identifikátory se používají k vytvoření identifikátorů zabezpečení, které jednoznačně identifikují objekty zabezpečení v dané doméně. Skutečný identifikátor zabezpečení vygenerovaný řadičem

domény se skládá z identifikátoru domény, který je stejný pro všechny objekty v dané doméně, a z jedinečného relativního identifikátoru, jenž objekty odlišuje od ostatních objektů v dané doméně.

Blok relativních identifikátorů vydaných pro řadič domény se nazývá fond RID. Řadiče domény, které byly nově propagované, musí získat fond RID před tím, než budou moci oznamovat svou dostupnost klientům služby Active Directory, nebo než budou moci sdílet složku SYSVOL. Stávající řadiče domény vyžadují další alokaci relativních identifikátorů, aby mohly pokračovat ve vytváření objektů zabezpečení poté, co se jejich aktuální fond RID vyčerpá. Jelikož relativní identifikátory jsou dlouhé 30 bitů, v doméně služby Active Directory je možno vytvořit nejvýše 1 073 741 824 (2^{30}) objektů zabezpečení. Po vyčerpání fondu RID na úrovni domény nebudou v dané doméně vytvořeny žádné nové objekty zabezpečení.

Obvykle se bloky relativních identifikátorů vydávají v počtu 500. Řadič domény začne požadovat nový fond po vyčerpání 250 (tj. 50 procent z 500) relativních identifikátorů. Úlohou hlavního serveru RID je vydávat bloky relativních identifikátorů a tuto úlohu provádí tehdy, pokud běží. Pokud se řadič domény nemůže připojit k hlavnímu serveru RID a z jakéhokoliv důvodu vyčerpá relativní identifikátory, na daném řadiči domény nebude možné vytvořit žádné nové objekty a vytvoření objektů skončí neúspěchem. Do protokolu Adresářová služba (Directory Service) na řadiči domény, který nemůže získat nové fondy RID, se zaznamená událost s ID 16645 a případně událost s ID 16651. Text zpráv uvedených událostí je následující:

Událost s ID 16645 – Byl přiřazen nejvyšší povolený počet identifikátorů účtů, přidělený pro tento řadič domény. Řadiči domény se nepodařilo získat nový fond identifikátorů. Řadič domény se pravděpodobně nemohl spojit s hlavním řadičem domény. Na tomto řadiči domény nebude možné vytvářet účty, dokud nezíská potřebný fond. Je možné, že se v doméně vyskytly potíže se síťovým spojením nebo je hlavní řadič domény offline či se v doméně nenachází. Ověřte, zda je hlavní řadič domény spuštěn a připojen do domény.

Událost s ID 16651 – Požadavek na nový fond identifikátorů účtů se nezdařil. Systém bude operaci opakovat, dokud neproběhne úspěšně. Nastala chyba %n %1.

Chcete-li tento problém vyřešit, je třeba zpřístupnit hlavní server RID, nebo je třeba přenést roli hlavního serveru RID na jiný server.

Z praxe: Ke zvýšení velikosti fondu RID lze použít nastavení RID Block Size v registru. Zvýšení fondu RID umožní každému řadiči domény vytvořit větší počet objektů zabezpečení bez kontaktování hlavního operačního serveru RID. I když změnu je nutno provést pouze na hlavním serveru RID, možná budete chtít nakonfigurovat tuto hodnotu na všech řadičích domény, pokud později přenesete roli hlavního operačního serveru RID na jiný řadič domény.

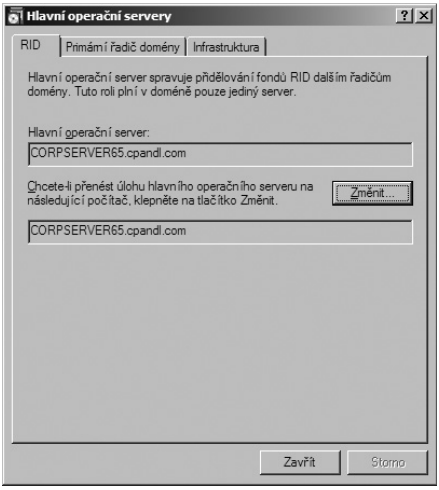
Nastavení RID Block Size používá hlavní operační server RID ke zjištění, jakou velikost fondu RID má vrátit žádajícímu řadiči domény. Nastavení RID Block Size obsahuje hod-

notu typu REG_DWORD a nachází se ve větvi HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\RID Values.

Systém Windows Server vytvoří nastavení RID Block Size automaticky a výchozí hodnotou je 0. Za těchto okolností se použije interní výchozí hodnota 500. Nastavení této hodnoty na hodnotu menší než 500 nemá žádný efekt a stále bude použita výchozí hodnota. Jelikož se neuplatňuje žádná maximální hodnota bloku, hodnota, která je příliš velká, může mít na doménu velmi nepříznivý vliv. Proč? Pokud alokujete relativní identifikátory ve velmi velkých blocích, některé řadiče domény mohou relativní identifikátory vyčerpat a nemusí být schopny získat nové relativní identifikátory, zatímco jiné domény mohou obsahovat velký počet nevyužitých relativních identifikátorů. Navíc, při každém vyřazení řadiče domény z provozu prostřednictvím přirozené nebo vynucené degradace nebo kvůli selhání hardwaru tento řadič přijde o všechny své relativní identifikátory. Podobně, při každém obnovení řadiče domény ze zálohy jsou všechny jeho relativní identifikátory zneplatněny, aby se podařilo zabránit tomu, aby byl jednomu uživatelskému účtu přiřazen stejný relativní identifikátor.

Hlavní server RID můžete vyhledat pomocí následujících kroků:

1. Spusťte nástroj Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) z nabídky Nástroje pro správu (Administrative Tools).
2. Pokud doména, se kterou chcete pracovat, není již zobrazena, klepněte pravým tlačítkem myši na uzlu Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) a poté zvolte příkaz Změnit doménu (Change Domain). V dialogovém okně Změnit doménu (Change Domain) zadejte název DNS domény, se kterou chcete pracovat, například **cs.cpandl.com**, a poté klepněte na tlačítko OK.
3. Klepněte pravým tlačítkem myši na doméně, se kterou chcete pracovat, a poté zvolte příkaz Hlavní operační servery (Operations Masters).
4. V dialogovém okně Hlavní operační servery (Operations Masters) se na kartě RID zobrazí aktuální hlavní server RID. (Viz obrázek 6.4.)



Obrázek 6.4: Vyhledejte hlavní server RID

Roli hlavního serveru RID můžete přenést na jiný server pomocí následujících kroků:

1. Spusťte nástroj Uživatelé a počítače služby Active Directory (Active Directory Users And Computers). Pokud doména, se kterou chcete pracovat, není již zobrazena, klepněte pravým

tlačítkem myši na uzlu Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) a poté zvolte příkaz Změnit doménu (Change Domain). V dialogovém okně Změnit doménu (Change Domain) zadejte název DNS domény, se kterou chcete pracovat, například **cs.cpandl.com**, a poté klepněte na tlačítko OK.

2. Klepněte pravým tlačítkem myši na uzlu domény a poté zvolte příkaz Změnit řadič domény (Change Domain Controller). V dialogovém okně Změnit adresářový server (Change Directory Server) zvolte možnost Tento řadič domény nebo instance služby AD LDS (This Domain Controller). Vyberte dostupný řadič domény, na který chcete přenést roli hlavního serveru RID, a poté klepněte na tlačítko OK.
3. Opět klepněte pravým tlačítkem myši na uzlu domény a poté zvolte příkaz Hlavní operační servery (Operations Masters). V dialogovém okně Hlavní operační servery (Operations Masters) vyberte kartu RID. Název aktuálního hlavního serveru RID se objeví v prvním textovém poli. Řadič domény, na který chcete přenést roli hlavního serveru RID, by se měl objevit ve druhém textovém poli. Pokud tomu tak není, zopakujte tuto proceduru počínaje krokem 1.
4. Klepněte na tlačítko Změnit (Change) a poté klepněte na tlačítko Zavřít (Close). Po vyzvání klepněte na tlačítko Ano (Yes) a potvrďte tak, že chcete přenést roli.
5. Po dokončení přenosu se zobrazí zpráva potvrzující přenos. Klepněte na tlačítko OK. Klepnutím na tlačítko Zavřít (Close) zavřete dialogové okno Hlavní operační servery (Operations Masters).

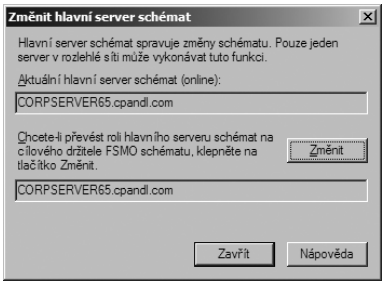
Správa hlavních serverů schémat

Hlavní server schémat je jediným řadičem domény v doménové struktuře se zapisovatelnou kopií kontejneru schématu. To znamená, že se jedná o jediný řadič domény v doménové struktuře, na kterém můžete provádět změny schématu. Změny schématu se provádí pomocí modulu snap-in Schéma služby Active Directory (Active Directory Schema). Po spuštění modulu snap-in Schéma služby Active Directory (Active Directory Schema) se vytvoří přímé spojení k hlavnímu serveru schémat, díky kterému si můžete prohlédnout schéma daného adresáře. Ovšem abyste mohli provádět změny schématu, musíte použít účet, který je členem skupiny Schema Admins.

Ve výchozím nastavení je hlavním serverem schémat první řadič domény nainstalovaný v kořenové doméně doménové struktury. Tuto roli můžete přenést pomocí modulu snap-in Schéma služby Active Directory (Active Directory Schema), nebo pomocí nástroje příkazové řádky NTDSUTIL.

Hlavní server schémat můžete vyhledat pomocí modulu snap-in Schéma služby Active Directory (Active Directory Schema) ve vlastní konzole. (Tipy k registraci a použití tohoto modulu najdete v části „Určení atributů pro replikaci“ v kapitole 5, „Konfigurace, údržba a řešení problémů se servery globálního katalogu“.) Po otevření tohoto modulu snap-in klepněte pravým tlačítkem myši na uzlu Schéma služby Active Direc-

tory (Active Directory Schema) a poté zvolte příkaz Hlavní operační server (Operations Master). V dialogovém okně Změnit hlavní server schémat (Change Schema Master), znázorněném na obrázku 6.5, se zobrazí aktuální hlavní server schémat.



Obrázek 6.5: Vyhledejte hlavní server schémat

Roli hlavního serveru schémat můžete přenést na jiný server pomocí následujících kroků:

1. Otevřete modul snap-in Schéma služby Active Directory (Active Directory Schema) ve vlastní konzole. Klepněte pravým tlačítkem myši na uzlu Schéma služby Active Directory (Active Directory Schema) a poté zvolte příkaz Změnit řadič domény služby Active Directory (Change Active Directory Domain Controller).
2. V dialogovém okně Změnit adresářový server (Change Directory Server) zvolte možnost Tento řadič domény nebo instance služby AD LDS (This Domain Controller). Do pole Vyhledat v této doméně (Look In This Domain) zadejte název kořenové domény doménové struktury a poté stiskněte klávesu Tab.
3. Dostupné řadiče domény se zobrazí podle lokality, typu a verze operačního systému. Vyberte dostupný řadič domény, na který chcete přenést roli hlavního serveru schémat, a poté klepněte na tlačítko OK.
4. Klepněte pravým tlačítkem myši na uzlu Schéma služby Active Directory (Active Directory Schema) a poté klepněte na příkaz Hlavní operační server (Operations Master). V dialogovém okně Změnit hlavní server schémat (Change Schema Master) se název aktuálního hlavního serveru schémat objeví v prvním textovém poli. Řadič domény, na který chcete přenést roli hlavního serveru schémat, by se měl objevit ve druhém textovém poli. Pokud tomu tak není, zopakujte tuto proceduru počínaje krokem 1.
5. Klepněte na tlačítko Změnit (Change) a poté klepněte na tlačítko Zavřít (Close). Po vyzvání klepněte na tlačítko Ano (Yes) a potvrďte tak, že chcete přenést roli.
6. Po dokončení přenosu se zobrazí zpráva potvrzující přenos. Klepněte na tlačítko OK. Klepnutím na tlačítko Zavřít (Close) zavřete dialogové okno Změnit hlavní server schémat (Change Schema Master).

Údržba hlavních operačních serverů

Jako správce budete provádět mnoho úloh, které vám pomohou s údržbou hlavních operačních serverů v celé doménové struktuře služby Active Directory. K rychlému obnovení hlavních operačních serverů si možná budete chtít připravit záložní hlavní operační servery. K zajištění správného fungování možná budete muset snížit vytížení hlav-

ního operačního serveru. V případě katastrofálního selhání možná budete muset vynuceně přenést roli hlavního operačního serveru.

Příprava záložních hlavních operačních serverů

Role hlavních operačních serverů jsou důležité pro správnou funkci doménové struktury a domény. Po instalaci služby Active Directory a vytvoření prvního řadiče domény v nové doménové struktuře je tomuto řadiči domény přiřazeno všech pět rolí. Po přidání domén jsou prvnímu řadiči domény, který nainstalujete do domény, automaticky přiřazeny role hlavního serveru RID, hlavního serveru infrastruktury a emulátoru primárního řadiče domény pro tuto doménu.

Pokud hlavní operační server přestane fungovat nebo se stane nedosažitelným, funkce, které hlavní operační server provádí, nebudou nadále dostupné, což by mohlo ochromit službu Active Directory. Abyste měli jistotu, že jste připraveni reagovat na selhání některého z hlavních operačních serverů, můžete označit další řadič domény jako záložní hlavní operační server. Záložní hlavní operační server je jednoduše řadič domény, kterému řeknete, že se má ujmout role hlavního operačního serveru v případě, že vlastník role selže.

Bude třeba určit zálohu pro role doménové struktury v kořenové doméně doménové struktury a zálohu pro role domény v každé doméně. Záloha by měla být optimálně připojena k aktuálnímu vlastníkovi role, který zajistí, že přenos role nastane co nejdříve a že v případě výpadku dojde k minimální ztrátě dat.

Kromě zajištění dostupnosti zálohy a jejího optimálního propojení s aktuálním hlavním operačním serverem nemusíte podniknout žádné další zvláštní kroky. To znamená, že můžete mezi záložním řadičem domény a hlavním operačním serverem vytvořit ruční objekt připojení, který zajistí přímou replikaci mezi těmito dvěma hlavními operačními servery. V tomto scénáři je ruční objekt připojení upřednostňován před automaticky vytvořeným objektem, protože služba Active Directory může automaticky vytvořené objekty připojení kdykoliv změnit, zatímco ručně vytvořená propojení zůstanou stejná, dokud je nezměníte. Přímé připojení pomáhá snížit pravděpodobnost možné ztráty dat v případě převzetí role, a tím pomáhá snížit pravděpodobnost poškození adresáře.

Poznámka: Pokud oddělíte role hlavních operačních serverů, stále můžete použít jeden záložní hlavní operační server pro doménovou strukturu a jeden hlavní operační server pro doménu. Ovšem měli byste zajistit, aby byl záložní hlavní operační server partnerským serverem pro replikaci se všemi vlastníky dané role.

Použitím účtu, který je členem skupiny Domain Admins nebo Enterprise Admins, můžete ručně vytvořit objekt připojení na hlavním operačním serveru a záložním hlavním operačním serveru, a to pomocí následujících kroků:

1. Spusťte modul Lokality a služby Active Directory (Active Directory Sites And Services) z nabídky Nástroje pro správu (Administrative Tools).

2. Rozbalte název lokality, v níž se nachází aktuální vlastník role hlavního operačního serveru, abyste rozbalili příslušnou složku Servers.
3. Rozbalte příslušnou složku Servers, abyste zobrazili seznam serverů ve vybrané lokalitě.
4. Vytvořte objekt příchozího připojení ze záložního serveru na aktuálním hlavním operačním serveru pomocí následujících kroků:
   A. Rozbalte název hlavního operačního serveru, na kterém chcete vytvořit objekt připojení, abyste zobrazili jeho objekt NTDS Settings.
   B. Klepněte pravým tlačítkem myši na objekt NTDS Settings, klepněte na příkaz Nová položka (New) a poté klepněte na příkaz Připojení (Connection).
   C. V dialogovém okně Najít - Řadiče domény služby Active Directory (Find Active Directory Domain Controllers) vyberte název partnerského serveru, ze kterého chcete vytvořit objekt připojení, a poté klepněte na tlačítko OK.
   D. V dialogovém okně Nový objekt - Připojení (New Object-Connection) zadejte příslušný název objektu připojení nebo přijměte výchozí název, a poté klepněte na tlačítko OK.
5. Rozbalte název lokality, v níž se nachází záložní server, abyste zobrazili odpovídající složku Servers.
6. Rozbalte příslušnou složku Servers, abyste zobrazili seznam serverů ve vybrané lokalitě.
7. Vytvořte objekt příchozího připojení z aktuálního serveru na záložním hlavním operačním serveru pomocí následujících kroků:
   A. Rozbalte název záložního serveru, na kterém chcete vytvořit objekt připojení, abyste zobrazili jeho objekt NTDS Settings.
   B. Klepněte pravým tlačítkem myši na objekt NTDS Settings, klepněte na příkaz Nová položka (New) a poté klepněte na příkaz Připojení (Connection).
   C. V dialogovém okně Najít - Řadiče domény služby Active Directory (Find Active Directory Domain Controllers) vyberte název aktuálního hlavního operačního serveru, ze kterého chcete vytvořit objekt připojení, a poté klepněte na tlačítko OK.
   D. V dialogovém okně Nový objekt - Připojení (New Object-Connection) zadejte příslušný název objektu připojení nebo přijměte výchozí název, a poté klepněte na tlačítko OK.

Vyřazení hlavních operačních serverů z provozu

Než trvale přepnete hlavní operační server do režimu offline, měli byste přenést všechny role hlavního operačního serveru, které obsahuje, na jiný řadič domény. Pokud použijete Průvodce instalací služby Active Directory Domain Services (Active Directory Domain Services Installation Wizard) k vyřazení řadiče domény, který je momentálně hostitelem jedné či více rolí hlavního operačního serveru, z provozu, průvodce automaticky znovu přiřadí tyto role jinému řadiči domény.

Abyste pochopili, jak tento proces funguje, uveďme si následující příklad:

1. Na řadiči domény spustíte Průvodce instalací služby Active Directory Domain Services (Active Directory Domain Services Installation Wizard) (Dcpromo). Průvodce po svém spuštění zjistí, zda je daný řadič domény momentálně hostitelem nějakých rolí hlavního operačního serveru.
2. Pokud nástroj Dcpromo nalezne nějaké role hlavního operačního serveru, požádá adresář o jiné vhodné řadiče domény a poté přenese role na některý z vhodných řadičů domény. Řadič domény je vhodný pro umístění rolí na úrovni domény, pokud je členem téže domény. Řadič domény je vhodný pro umístění role na úrovni doménové struktury, pokud je členem téže doménové struktury.

Jak můžete vidět, automatizovaný proces přenosu role vám neumožní zadat řadič domény, který by se měl ujat rolí hlavního operačního serveru. Proto pokud chcete, aby role hlavního operačního serveru byla nebo byly přiřazeny na konkrétní řadič domény, musíte tyto role přenést před vyřazením aktuálního vlastníka role z provozu.

Snížení zátěže hlavních operačních serverů

Hlavní operační servery se mohou přetížit, pokud se pokusí obsloužit klientské požadavky v síti, spravovat své vlastní prostředky a provádět své jedinečné úlohy hlavního operačního serveru. Pokud dojde k přetížení hlavního operačního serveru a ovlivní to jeho výkon, můžete změnit konfiguraci prostředí, aby některé úlohy byly prováděny jinými, méně využívanými řadiči domény. Bude-li třeba zpracovat méně klientských požadavků, hlavní operační server může použít více prostředků k provedení svých jedinečných funkcí v doménové struktuře či v doméně.

Pro snížení zátěže na hlavním operačním serveru vyhledejte nedůležité funkce a přesuňte je na jiné servery. Pokud přetížený hlavní operační server rovněž slouží jako server DNS nebo server globálního katalogu, můžete tyto funkce přesunout na jiné servery a snížit tak zatížení serveru.

Rovněž byste mohli přizpůsobit váhu řadiče domény v prostředí DNS tak, že bude zpracovávat méně klientských požadavků pro určitou službu. S méně požadavky na zpracování může daný řadič domény použít více prostředků k provedení služeb hlavního operačního serveru pro danou doménu. Například abyste nakonfigurovali emulátor primárního řadiče domény tak, aby přijímal pouze polovinu klientských požadavků

jako jiné řadiče domény, nastavte váhu záznamu LDAP SVR na hodnotu 50. Budeme-li předpokládat, že jiné řadiče domény mají stejnou prioritu a používají stejnou hodnotu váhy 100, služba DNS by pak určila poměr váhy pro emulátor primárního řadiče domény jako 50/100 (50 pro emulátor primárního řadiče domény a 100 pro ostatní řadiče domény). Po snížení tohoto poměru na hodnotu 50/100 bude služba DNS odkazovat klienty na jiné řadiče domény dvakrát častěji, než je odkazuje na emulátor primárního řadiče domény. Pokud snížíte odkazování klientů pro protokol LDAP, emulátor primárního řadiče domény přijme méně klientských požadavků a bude mít více prostředků na jiné úlohy, jako například na provádění úloh souvisejících s jeho rolí hlavního operačního serveru.

Z praxe: Nepleťte si váhu s prioritou. Abyste zabránili klientům v odesílání všech požadavků na jediný řadič domény, řadičům domény je přiřazena hodnota priority. Výchozí hodnotou je 0. Klient použije hodnotu priority ke snazšímu zjištění, na který řadič domény má odesílat požadavky. Pokud klient použije k nalezení řadiče domény službu DNS, klientovi se vrátí hodnota priority (stejně jako zbývající informace služby DNS potřebné k dokončení požadavku).

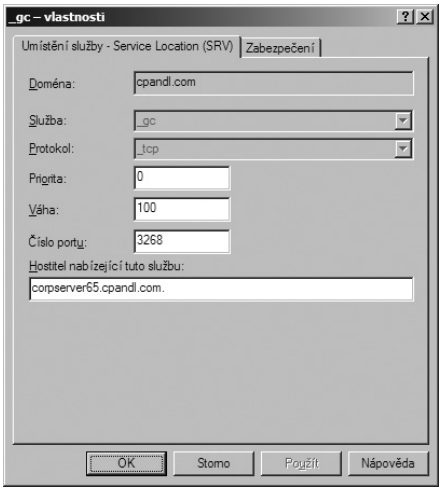
Klienti vždy odesílají požadavky řadiči domény, který má nejnižší hodnotu priority. Pokud má stejnou hodnotu více než jeden řadič domény, klienti si náhodně vyberou ze skupiny řadičů domény se stejnou hodnotou. Pokud nejsou dostupné žádné řadiče domény s nejnižší hodnotou priority, klienti odešlou požadavky řadiči domény s další-vyšší prioritou. Proto může zvýšení hodnoty priority záznamu o prostředku LDAP pro emulátor primárního řadiče domény snížit jeho pravděpodobnost na přijetí klientských požadavků.

Ovšem i když změna priority řadiče domény rovněž sníží počet klientských odkazů na daný řadič domény, změna může mít i nežádoucí vedlejší účinky. Spíše než rovnoměrné snížení přístupu k určitému řadiči domény vzhledem k jiným řadičům domény způsobí změna priority to, že služba DNS nebude na tento řadič domény odkazovat žádné klienty, pokud budou pořád dostupné řadiče domény s nastavením nižší priority.

Chcete-li změnit relativní prioritu a váhu pro určitou službu hlavního operačního serveru ve službě DNS, postupujte podle následujících kroků:

1. Klepněte na tlačítko Start, zvolte příkaz Nástroje pro správu (Administrative Tools) a poté klepněte na příkaz DNS.
2. Připojte se k řadiči domény v kořenové doméně doménové struktury. Klepněte pravým tlačítkem myši na objekt DNS, klepněte na příkaz Připojit k serveru DNS (Connect To DNS Server) a poté klepněte na příkaz V následujícím počítači (The Following Computer). Zadejte název řadiče domény v kořenové doméně doménové struktury a poté klepněte na tlačítko OK.
3. Rozbalte uzel Zóny dopředného vyhledávání (Forward Lookup Zones) a poté rozbalte kořenovou doménu doménové struktury.

4. Klepněte na kontejner _tcp. Záznamy _ldap řídí požadavky adresáře. Záznamy _gc řídí požadavky globálního katalogu. V podokně podrobností najděte záznam SRV _ldap nebo _gc, který obsahuje název hlavního operačního serveru. Datové pole zobrazí prioritu, váhu a číslo portu přiřazené danému záznamu o prostředku, stejně jako název serveru, ke kterému daný záznam patří.
5. Poklepejte pravým tlačítkem myši na záznamu o prostředku SRV, který chcete změnit. Tím zobrazíte dialogové okno s vlastnostmi pro daný záznam, jak můžete vidět na obrázku 6.6.
6. Podle potřeby použijte pole Priority k zadání relativní priority hostitele s ohledem na ostatní hostitele v doméně, které nabízí stejnou službu. Nejvyšší prioritu má hostitel, který obsahuje hodnotu priority nastavenou na 0. Pokud mají dva či více hostitelů stejnou prioritu, k určení, který hostitel se má použít, lze použít váhu.
7. Podle potřeby použijte pole Váha (Weight) k zadání relativní váhy hostitele a k rozložení zátěže dané služby. Pokud mají dva či více hostitelů určité služby stejnou prioritu, pomocí váhy lze nastavit přednost jednoho hostitele před druhým. Hostitelé s vyšší váhou by se měli použít jako první.



Obrázek 6.6: *Podle potřeby nastavte prioritu a váhu*

8. Klepnutím na tlačítko OK uložte změny. Změny budou rozptýleny na ostatní servery DNS během pravidelných operací přenosu zóny. V závislosti na konfiguraci služby DNS může tento proces trvat několik dnů.

Upozornění: Neměňte záznamy lokátorů služeb bez pečlivého plánování s přihlédnutím k potenciálnímu dopadu na vaši síť. Po změně záznamů lokátorů služeb bude třeba pečlivě sledovat vaši síť, aby byla zaručená její bezchybná funkčnost.

Převzetí rolí hlavního operačního serveru

V případě selhání hlavního operačního serveru se musíte rozhodnout, zda potřebujete přemístit roli hlavního operačního serveru na jiný řadič domény, nebo zda vyčkáte, než bude daný řadič domény opět funkční. Své rozhodnutí můžete založit na nezbytnosti role, kterou daný řadič domény hostí, a na očekávané době výpadku.

Pokud hlavní operační server selže a nevrací se zpět do režimu online, je třeba převzít roli a vynutit její přenos na jiný řadič domény. Převzetí role je drastický krok, který byste měli provést, pouze pokud předchozí vlastník role nebude nikdy znovu dostupný. Nepřebírejte roli hlavního operačního serveru, pokud ji můžete řádně přenést prostřednictvím běžné procedury přenosu. Převzetí role by mělo být posledním krokem.

Příprava na převzetí rolí hlavního operačního serveru

Před převzetím role a jejím vynuceným převzetím byste měli zjistit, do jaké míry je řadič domény, který převezme danou roli, aktuální ve srovnání s předchozím vlastníkem role. Služba Active Directory sleduje změny replikace prostřednictvím čísel pořadí aktualizace USN (update sequence numbers). Kvůli zpoždění replikace nemusí být všechny řadiče domény aktuální. Pokud porovnáte číslo USN řadiče domény s čísly USN jiných serverů v doméně, můžete zjistit, zdali je daný řadič domény nejaktuálnější, pokud jde o změny od předchozího vlastníka role. Pokud je daný řadič domény aktuální, můžete roli bezpečně přenést. Pokud řadič domény aktuální není, můžete počkat na replikaci a poté přenést roli na řadič domény.

Systém Windows Server 2008 obsahuje nástroj Repadmin pro práci s replikací služby Active Directory. Chcete-li zobrazit nejvyšší pořadové číslo pro zadaný názvový kontext na každém partnerském serveru pro replikaci určeného řadiče domény, zadejte v příkazovém řádku následující příkaz.

```
repadmin /showutdvec Název_řadiče_domény Názvový_kontext
```

Zde je *Název_řadiče_domény* plně kvalifikovaný název domény daného řadiče domény a *Názvový_kontext* je rozlišující název domény, v níž se daný server nachází, jako v následujícím vzorovém kódu.

```
repadmin /showutdvec corpserver52 dc=cpandl,dc=com
```

Následující výstup zobrazuje nejvyšší číslo USN na partnerských serverech pro replikaci pro daný oddíl domény.

```
Hlavní-Lokalita\corpserver31    @ USN    678321 @ Čas 2008-03-15 12:42:32
Hlavní-Lokalita\corpserver26    @ USN    681525 @ Čas 2008-03-15 12:42:35
```

V tomto příkladě platí, že pokud byl server CorpServer31 předchozím vlastníkem role a ověřovaný řadič domény má stejné nebo vyšší číslo USN pro server CorpServer31, řadič domény je aktuální. Ovšem pokud server CorpServer31 byl předchozím vlastníkem role a ověřovaný řadič domény měl nižší číslo USN pro server CorpServer31, řadič domény aktuální není, a vy byste měli před převzetím role počkat na replikaci. Rovněž byste mohli použít příkaz Repadmin /Syncall k tomu, abyste řadič domény, který je nejaktuálnější vzhledem k předchozímu vlastníkovi role, donutili provést replikaci se všemi jeho partnerskými servery pro replikaci.

Převzetí rolí hlavního operačního serveru

Převzít roli hlavního operačního serveru můžete pomocí následujících kroků:

1. Otevřete příkazový řádek na konzole serveru, který chcete přiřadit jako nový hlavní operační server. To můžete provést místně nebo pomocí nástroje Připojení ke vzdálené ploše (Remote Desktop).
2. Vypište aktuální hlavní operační servery zadáním příkazu **netdom query fsmo**.
3. Zadejte příkaz **ntdsutil**. V příkazovém řádku nástroje ntdsutil zadejte příkaz **roles**.
4. V příkazovém řádku nástroje fsmo maintenance zadejte příkaz **connections**.
5. V příkazovém řádku nástroje server connections zadejte příkaz **connect to server** následovaný plně kvalifikovaným názvem domény řadiče domény, kterému chcete přiřadit roli hlavního operačního serveru.
6. Po vytvoření připojení k řadiči domény ukončete příkazový řádek nástroje server connections zadáním příkazu **quit**.
7. V příkazovém řádku nástroje fsmo maintenance zadejte jeden z následujících příkazů:
   - seize pdc
   - seize rid master
   - seize infrastructure master
   - seize schema master
   - seize domain name master
8. V příkazovém řádku nástroje fsmo maintenance zadejte příkaz **quit**.
9. V příkazovém řádku nástroje ntdsutil zadejte příkaz **quit**.

Po převzetí role hlavního operačního serveru budete muset odebrat příslušná data z Active Directory. (Další informace najdete v části „Provedení vynuceného odebrání řadičů domény“ a „Vyčištění metadat v doménové struktuře služby Active Directory“ v kapitole 3, „Nasazení řadičů domény s možností zápisu“.)

Řešení problémů s hlavními operačními servery

Všechny řadiče domény, včetně hlavních operačních serverů, replikují data vzájemně mezi sebou. Replikace představuje míru, do jaké jsou řadiče domény aktuální ve srovnání se změnami adresáře. Součástí diagnostiky a řešení problémů s hlavními operačními servery je požadavek na zajištění pravidelnosti replikace. Obecně lze říci, že čím větší a rozsáhlejší je prostředí služby Active Directory, tím déle trvá úplná replikace změn na všechny řadiče domény.

Řadu automatizovaných testů můžete na hlavním operačním serveru spustit pomocí nástroje Dcdiag pomocí následujících kroků:

1. Spusťte příkazový řádek se zvýšeným oprávněním správce klepnutím na tlačítko Start, klepnutím pravým tlačítkem myši na příkazu Příkazový řádek (Command Prompt) a poté klepnutím na příkazu Spustit jako správce (Run As Administrator).
2. V příkazovém řádku se zvýšeným oprávněním zadejte následující příkaz: **dcdiag /s:*Název_serveru*** kde *Název_serveru* označuje název hlavního operačního serveru, který chcete ověřit. Pokud jste k hlavnímu operačnímu serveru již přihlášeni, jednoduše zadejte příkaz **dcdiag** bez dalších parametrů.
3. Zkontrolujte stav všech testů. Pokud některý test selže, poznamenejte si test, který selhal, a podnikněte příslušné nápravné kroky.

Poznámka: Nástroj Dcdiag můžete spustit bez použití příkazového řádku se zvýšeným oprávněním správce. Ovšem pokud tak učiníte, obdržíte nepřesné výsledky testů, neboť testy vyžadující zvýšené oprávnění selžou.

Použitím příkazového řádku se zvýšeným oprávněním správce můžete ověřit, zda se hlavní operační server úspěšně replikuje s ostatními řadiči domény. V příkazovém řádku se zvýšeným oprávněním zadejte následující příkaz: **repadmin /showrepl *Název_serveru***, kde *Název_serveru* označuje název hlavního operačního serveru, který chcete ověřit. Pokud jste k hlavnímu operačnímu serveru již přihlášeni, jednoduše zadejte příkaz **repadmin /showrepl**.

Nástroj Repadmin poté vypíše příchozí sousedy pro aktuální nebo zadaný řadič domény. Tito příchozí sousedé rozpoznají rozlišující název každého oddílu adresáře, pro který byl učiněn pokus o příchozí replikaci adresáře, lokalitu a název zdrojového řadiče domény a to, zdali byla replikace úspěšná.

Krom toho, i když je emulátor primárního řadiče domény obvykle časovým serverem pro doménovou strukturu, kterýkoliv správce mohl tuto konfiguraci změnit. Abyste zjistili, zdali je emulátor primárního řadiče domény výchozím zdrojem času služby Systémový čas (Windows Time) (W32time) pro danou doménovou strukturu, můžete použít nástroj Nltest. V příkazovém řádku zadejte následující příkaz: **nltest /server:*Název_serveru* /dsgetdc:*Název_domény***, kde *Název_serveru* označuje název emulátoru primárního řadiče domény a *Název_domény* označuje název domény, do které daný server patří. V následujícím příkladě můžete ověřit server CentralDC89 v doméně cpandl.com.

```
nltest /server:centraldc89 /dsgetdc:cpandl.com
```

Výstup bude vypadat nějak podobně.

```
           Řadič domény: \\CENTRALDC89.cpandl.com
                 Adresa: \\192.168.15.122
            Guid domény:
           Název domény: cpandl.com
Název doménové struktury: cpandl.com
```

```
Název sítě řadiče domény: Atlanta-Lokalita-1
         Název naší sítě: NY-Lokalita-1
                Příznaky: PDC GC DS LDAP KDC TIMESERV GTIMESERV ZAPISOVATELNÉ
DOMÉNOVÁ_STRUKTURA_DNS UKONČIT_SÍŤ ÚPLNÝ_TAJNÝ_KLÍČ
Příkaz byl úspěšně dokončen.
```

Pokud se v řádku Příznaky (Flags) uvedeného výstupu objeví řetězec PDC, jako ve výstupu výše uvedeného příkladu, pak je řadič domény emulátorem primárního řadiče domény. Pokud se objeví řetězec GTIMESERV, pak je řadič domény globálním časovým serverem pro danou doménovou strukturu.