KAPITOLA 17

Správa služby Active Directory

Po dokončení instalace a počáteční konfiguraci vašeho prostředí služby Active Directory zjistíte, že se vaše pracovní vytížení podstatně snížilo. Je-li služba Active Directory správně nainstalována, je velmi stabilní a vyžaduje jen málo denní údržby. Ovšem je třeba pravidelně provádět určité úlohy. Mezi ně patří správa databáze služby AD DS a rolí řadiče domény a zajištění vhodného odpovídajícího procesu zotavení po havárii.

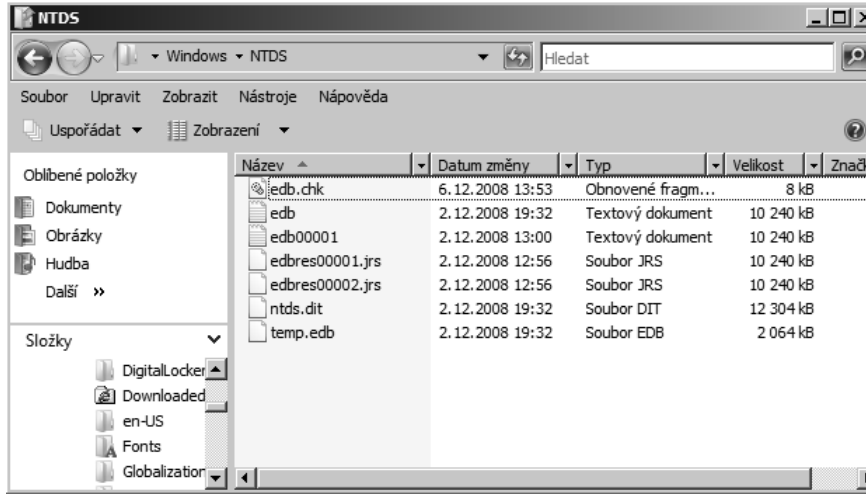
Správa databáze služby AD DS

Jednou z nejdůležitějších součástí správy služby AD DS je údržba databáze služby AD DS. Za běžných okolností budete jen zřídkakdy spravovat databázi služby AD DS přímo, neboť pravidelná, automatická správa databáze zajistí dobrý stav vaší databáze ve všech situacích, kromě těch mimořádných. Tyto automatické procesy zahrnují online defragmentaci databáze služby AD DS i proces uvolnění paměti, zajišťující vyčištění odstraněných položek. Pro výjimečné příležitosti, kdy potřebujete spravovat databázi služby AD DS, systém Windows Server 2008 nabízí nástroj Ntdsutil.

Úložiště dat služby AD DS

Databáze služby AD DS je uložena v souboru s názvem Ntds.dit, který se ve výchozím nastavení nachází ve složce %systemroot%\NTDS. Obsah této složky je znázorněn na obrázku 17.1. Tato složka rovněž obsahuje následující soubory:

- **Edb.chk** – tento soubor je kontrolním souborem, který indikuje, které transakce ze souborů protokolů byly zapsány do databáze služby AD DS.
- **Edb.log** – tento soubor je skutečným protokolem transakcí. Tento soubor protokolu má neměnnou velikost, přesně 10 MB.
- **Edbxxxxx.log** – po chvíli spuštění služby AD DS můžete mít jeden nebo více souborů protokolu, jejichž část *xxxxx* názvu souboru je hodnotou, která se zvyšuje po šestnáctkových číslech. Tyto soubory protokolů jsou předchozí soubory protokolů; když se aktuální soubor protokolu zaplní, přejmenuje se na nejbližší předchozí soubor protokolu a vytvoří se nový soubor Edb.log. Staré soubory protokolů se automaticky odstraní, jakmile jsou změny v souborech protokolů provedeny v databázi služby AD DS. Každý z těchto souborů protokolu má rovněž velikost 10 MB.
- **Edbtmp.log** – tento protokol je dočasným protokolem, který se použije, jakmile se aktuální soubor protokolu (Edb.log) zaplní. Vytvoří se nový soubor s názvem Edbtemp.log, v němž jsou uloženy všechny transakce, a soubor Edb.log se přejmenuje na nejbližší předchozí soubor protokolu. Poté je soubor Edbtmp.log přejmenován na soubor Edb.log. Jelikož použití tohoto názvu souboru je přechodné, typicky není viditelný.
- **Edbres00001.jrs a edbres00002.jrs** – tyto soubory jsou vyhrazené soubory protokolů, které se používají, pouze pokud na pevném disku, jenž obsahuje soubory protokolů, dojde volné místo. Pokud se aktuální soubor protokolu zaplní a server nemůže vytvořit nový soubor protokolu, jelikož na pevném disku už není žádné volné místo, server vyprázdní všechny transakce služby AD DS, které se zrovna nachází v paměti,



Obrázek 17.1: Soubory služby AD DS jsou umístěny ve složce %systemroot%\NTDS

do těchto dvou vyhrazených souborů protokolu a poté ukončí službu AD DS. Oba tyto soubory protokolu mají rovněž velikost 10 MB.

- **Temp.edb** – tento dočasný soubor se používá během údržby databáze a k uložení informací o právě zpracovávaných transakcích.

Uvolnění mezipaměti

Jedním z automatických procesů používaných ke správě databáze služby AD DS je uvolnění paměti (garbage collection). Uvolnění mezipaměti je proces, který se spustí na každém řadiči domény každých 12 hodin. Během procesu uvolnění mezipaměti se znovu získá volné místo v databázi služby AD DS.

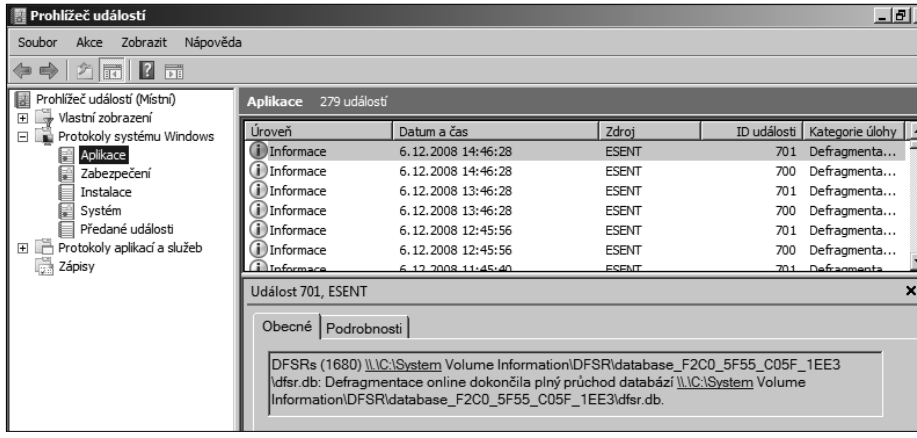
Proces uvolnění mezipaměti je zahájen nejprve odstraněním objektů označených jako neplatné z databáze. *Objekty označené jako neplatné* jsou pozůstatky objektů, které byly smazány ze služby AD DS. Pokud dojde k odstranění objektu jako například uživatelský účet, objekt není odstraněn okamžitě. Místo toho je v objektu nastaven atribut *isDeleted* na hodnotu *True*, objekt je označen jako neplatný a většina atributů tohoto objektu je z objektu odstraněna. Tento objekt označený jako neplatný je poté replikován na ostatní řadiče domény v dané doméně. Každý řadič domény udržuje kopii objektu označeného jako neplatný, dokud nevyprší jeho životnost. Ve výchozím nastavení je životnost objektu označeného jako neplatný nastavena na 180 dnů. Při příštím spuštění procesu uvolnění mezipaměti po vypršení životnosti objektu označeného jako neplatný je tento objekt z databáze odstraněn.

Online defragmentace

Posledním krokem procesu uvolnění mezipaměti je online defragmentace databáze služby AD DS. Tato online defragmentace uvolní místo v databázi a přeuspořádá úložiště objektů služby AD DS v databázi, čímž zvýší efektivitu databáze. Během běžného provozu je databázový systém služby AD DS optimalizován tak, aby umožnil co nejrychlejší provádění změn databáze služby AD DS. Při odstranění objektu ze služby AD DS je stránka databáze, v níž je daný objekt uložen, načtena do paměti počítače a objekt je z dané stránky odstraněn. Jakmile jsou objekty přidány do služby AD DS, jsou zapsány do stránek databáze bez ohledu na optimalizaci úložiště těchto informací pro pozdější načtení. Po několika hodinách co nejrychlejšího možného provádění změn v databázi nemusí být úložiště dat v databázi optimalizováno. Databáze by například mohla obsahovat prázdné stránky, v nichž byly objekty odstraněny, může existovat mnoho stránek s některými odstraněnými položkami nebo by mohly být objekty služby AD DS, které by měly být logicky uloženy pohromadě, uloženy v mnoha různých stránkách v databázi.

Proces online defragmentace vyčistí databázi a vrátí ji do optimalizovanějšího stavu. Jedno z omezení procesu online defragmentace spočívá v tom, že se při tomto procesu nezmenší velikost databáze služby AD DS. Pokud jste z databáze služby AD DS odstranili velký počet objektů, proces online defragmentace by mohl vytvořit mnoho prázdných stránek v databázi, neboť došlo k přesunu objektů v databázi. Ovšem proces online defragmentace nedokáže odstranit tyto prázdné stránky z databáze. K odstranění těchto stránek musíte použít proces offline defragmentace.

Proces online defragmentace se spouští každých 12 hodin jako součást procesu uvolnění mezipaměti. Po dokončení procesu online defragmentace je do protokolu adresářové služby zapsána událost indikující úspěšné dokončení procesu. Obrázek 17.2 znázorňuje příklad takovéto zprávy události protokolu.



Obrázek 17.2: Zpráva adresářové služby v protokolu Aplikace indikující úspěšnou online defragmentaci

Služba Active Directory Domain Services s možností restartu

Na rozdíl od předchozích verzí služby Active Directory služba AD DS v systému Windows Server 2008 může být zastavena a restartována při spuštěném počítači. Pokud v předchozích verzích správce chtěl spustit řadič domény bez načtení služby AD DS, server bylo třeba restartovat v Režimu obnovení adresářových služeb (Active Directory Restore Mode). Tím by se spustil server jako samostatný server bez služby AD DS. Poté byste mohli provádět úlohy offline údržby, například offline defragmentaci nebo přesunutí databáze a souborů protokolu. V případě systému Windows Server 2008 může být adresářová služba přepnuta do režimu offline, zatímco počítač stále běží, s minimálním ovlivněním ostatních služeb.

Tři možné stavy služby AD DS na řadiči domény se systémem Windows Server 2008 jsou popsány v tabulce 17.1.

Zastavením služby AD DS můžete provádět některé úlohy správy databáze. Mezi tyto úlohy patří:

- Provádění offline defragmentace
- Přesunutí databáze služby AD DS nebo souborů protokolu

Důležité: Nemůžete obnovit databázi služby AD DS, pokud je služba AD DS zastavena. Abyste mohli provést obnovení, musíte server restartovat do Režimu obnovení adresářových služeb (Directory Services Restore Mode).

Tabulka 17.1: Možné stavy služby AD DS

Stav	Popis
Služba AD DS spuštěna	V tomto stavu je služba AD DS spuštěna. Pro klienty a ostatní služby běžící na serveru je řadič domény se systémem Windows Server 2008 běžící v tomto stavu stejný jako řadič domény běžící se systémem Windows 2000 Server nebo Windows Server 2003.
Služba AD DS zastavena	V tomto stavu je služba AD DS zastavena. Ačkoliv je tento režim unikátní, server má některé charakteristiky řadiče domény v režimu Restore Mode služby Active Directory i členského serveru připojeného k doméně. Podobně jako u režimu obnovení adresářové služby je databáze služby AD DS (Ntds.dit) na místním řadiči domény v režimu offline. Jiný řadič domény může být kontaktován pro přihlašování, pokud je nějaký dostupný. Pokud nelze kontaktovat žádný jiný řadič domény, můžete pro přihlášení k místnímu řadiči domény použít heslo režimu obnovení adresářové služby.
Režim obnovení adresářových služeb (Directory Services Restore Mode)	V tomto režimu je služba AD DS v režimu offline a správce se musí přihlásit k počítači pomocí hesla režimu obnovení adresářové služby. Zásady domény nejsou na server použity.

Pokud chcete službu AD DS zastavit, spusťte ze složky Nástroje pro správu (Administrative Tools) konzolu Služby (Services) pro správu služeb. Poté klepněte pravým tlačítkem myši na službě Active Directory Domain Services a zvolte příkaz Zastavit (Stop). Zapamatujte si, že zastavením služby AD DS zastavíte také následující závislé služby:

- Služba KDC (Key Distribution Center) protokolu Kerberos (Kerberos Key Distribution Center) (KDC)
- Zasílání zpráv mezi lokalitami (Intersite Messaging)
- Služba replikace souborů (File Replication Service (FRS))
- Server DNS (DNS Server)

Offline defragmentace databáze služby AD DS

Jak jsme zmínili už dříve, proces online defragmentace nezmenší velikost databáze služby AD DS. Za normálních okolností v tom není žádný problém, neboť stránky databáze, které jsou během online defragmentace vyčištěny, se jednoduše znovu použijí při přidání nových objektů do služby AD DS. Ovšem v některých případech byste mohli chtít použít offline defragmentaci, abyste zmenšili celkovou velikost databáze. Například pokud odstraníte globální katalog z řadiče domény, měli byste spustit offline defragmentaci databáze, abyste vyčistili místo použité v databázi k uložení informací o globálním katalogu. Tato potřeba offline defragmentace platí obzvlášť v prostředí s více doménami, v němž může být globální katalog značně velký. Rovněž byste mohli chtít použít offline defragmentaci, pokud jste přesunuli velký počet objektů z domény služby AD DS.

Chcete-li spustit offline defragmentaci, postupujte podle následujících kroků:

1. Proveďte zálohu informací o službě AD DS na řadiči domény. Tento proces je popsán dále v této kapitole.
2. Otevřete konzolu Služby (Services) a zastavte službu Active Directory Domain Services a všechny související služby, které budou potřeba (nebo zadejte na příkazovém řádku příkaz net stop ntds).

3. Otevřete příkazový řádek a zadejte příkaz ntdsutil.
4. Na příkazovém řádku Ntdsutil zadejte příkaz activate instance NTDS.
5. Na příkazovém řádku Ntdsutil zadejte příkaz files.
6. Na příkazovém řádku File Maintenance zadejte příkaz info. Tato možnost zobrazí aktuální informace o cestě a velikosti databáze služby AD DS a jejích souborů protokolu.
7. Zadejte příkaz compact to jednotka:\adresar. Vyberte jednotku a adresář, které mají dostatek místa k uložení celé databáze. Pokud název cesty k adresáři obsahuje mezery, cesta musí být uzavřena v uvozovkách.
8. Proces offline defragmentace vytvoří novou databázi s názvem Ntds.dit ve vámi zadané cestě. Zkopírováním databáze do nového umístění dojde k její defragmentaci.
9. Po dokončení defragmentace zadejte dvakrát příkaz quit pro návrat na příkazový řádek.
10. Zkopírujte defragmentovaný soubor Ntds.dit přes původní soubor Ntds.dit v cestě k databázi služby AD DS a odstraňte staré soubory protokolů.
11. Restartujte službu Active Directory Domain Services.

Poznámka: Pokud defragmentujete databázi proto, že jste odstranili velký počet objektů ze služby AD DS, musíte tuto proceduru zopakovat na všech řadičích domény.

Přesunutí databáze a umístění protokolu transakcí

Nástroj Ntdsutil lze rovněž použít k přesunutí databáze služby AD DS a souborů transakcí. Například pokud se soubory protokolů a databáze nachází na stejném pevném disku, mohli byste chtít přesunout jednu ze součástí na jiný pevný disk. Pokud se pevný disk obsahující soubor databáze zaplní, budete muset databázi přesunout.

Chcete-li přesunout databázi a protokol transakcí do nových umístění na serveru v Režimu obnovení adresářových služeb (Directory Services Restore Mode) (nebo se zastavenou službou Active Directory Domain Services), postupujte podle následujících kroků:

1. Otevřete příkazový řádek a zadejte příkaz ntdsutil.
2. Na příkazovém řádku Ntdsutil zadejte příkaz activate instance NTDS.
3. Na příkazovém řádku Ntdsutil zadejte příkaz files.
4. Abyste zjistili aktuální umístění souborů, zadejte na příkazovém řádku Ntdsutil příkaz info. Tento příkaz vypíše seznam umístění databáze a všech protokolů.
5. Chcete-li přesunout soubor databáze, na příkazovém řádku file maintenance zadejte příkaz move db to adresar, kde adresar je cílovým umístěním souborů. Tento příkaz přesune databázi do zadaného umístění a překonfigurujte registr, aby měl přístup k souboru ve správném umístění.

6. Pro přesunutí protokolů transakcí zadejte na příkazovém řádku file maintenance příkaz move logs to adresar.
7. Restartujte server nebo službu AD DS.

Zálohování služby AD DS

Proces zálohování služby AD DS v systému Windows Server 2008 se liší od procesu používaného v systémech Windows Server 2003 a Windows 2000 Server. Program Zálohování serveru (Windows Server Backup) a nástroj Wbadmin.exe nahrazují předchozí nástroj pro zálohování Ntbackup.exe. Nový nástroj pro zálohování doznal následujících změn:

- Program Zálohování serveru (Windows Server Backup) a nástroj Wbadmin.exe se ve výchozím nastavení neinstalují. Pokud chcete používat tyto nástroje, musíte nainstalovat funkce Zálohování serveru (Windows Server Backup) a Nástroje příkazového řádku (Command-line Tools). Při instalaci nástrojů příkazového řádku se rovněž nainstaluje funkce Prostředí Windows Powershell (Windows PowerShell).
- Zálohovat lze pouze celé svazky. Program Zálohování serveru (Windows Server Backup) neumožňuje zálohovat pouze data o stavu systému, touto možností disponuje služba AD DS. V případ programu Zálohování serveru (Windows Server Backup) musíte zálohovat všechny kritické svazky, abyste zazálohovali data o stavu systému.

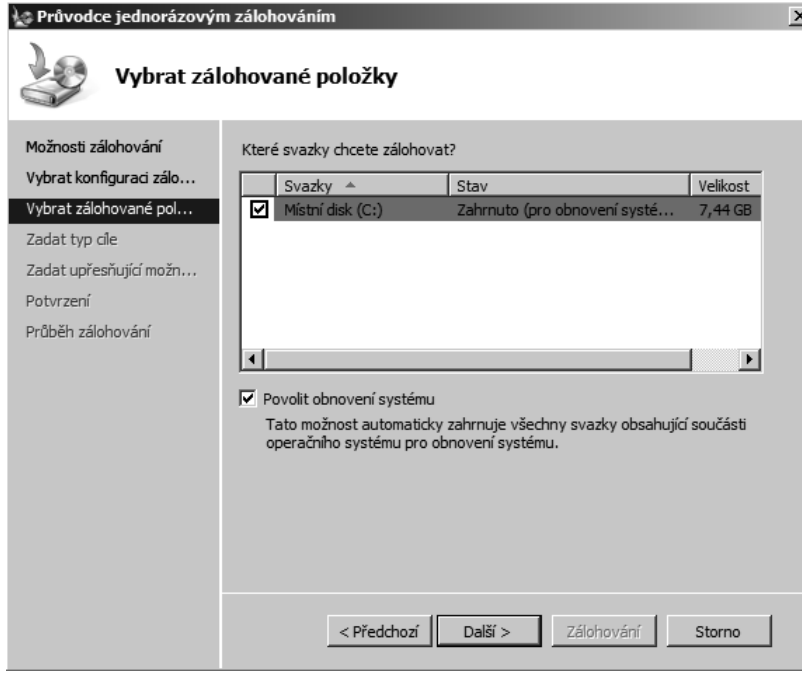
Poznámka: Informace o stavu systému na řadiči domény můžete zálohovat pouze pomocí nástroje příkazového řádku Wbadmin.exe. Obecnou praxí však je, aby zálohování všech systémových svazků bylo součástí všeho pravidelného procesu zálohování.

- Zálohy se provedou pouze na disk nebo disk DVD. Program Zálohování serveru (Windows Server Backup) neprovádí zálohování na pásku. Pokud chcete zálohovat na pásku, musíte použít zálohovací řešení od jiného výrobce. Zálohy můžete uložit na místní disk, externí disk, vzdálenou sdílenou složku nebo na disk DVD.

Data o stavu systému jsou kolekcí konfiguračních dat na serveru. Tato data jsou úzce integrována a musí být zálohována a obnovena jako jeden celek. V systému Windows Server 2008 při použití programu Zálohování serveru (Windows Server Backup) musíte zazálohovat kritické svazky obsahující data o stavu systému. V programu Zálohování serveru (Windows Server Backup) se možnost Povolit obnovení systému (Enable System Recovery) používá k automatickému výběru všech nepostradatelných svazků, viz obrázek 17.3.

Kritické svazky serveru se liší v závislosti na rolích instalovaných na serveru. Systémový svazek obsahuje spouštěcí soubory, například úložiště konfiguračních dat spouštění a soubor Bootmgr, a je nepostradatelným svazkem. Spouštěcí svazek s operačním systémem Windows je rovněž nepostradatelným svazkem. Systémy obsahující následující další data jsou rovněž nepostradatelnými svazky:

- adresář SYSVOL
- databáze služby AD DS a soubory protokolů
- registr



Obrázek 17.3: Pomocí programu Zálohování serveru (Windows Server Backup) proveďte zálohu všech nepostradatelných svazků

- registrační databáze tříd modelu COM+
- databáze služby Active Directory Certificate Services
- informace o službě Cluster
- systémové soubory, které jsou pod ochranou programu Windows Resource Protection

Poznámka: Členové skupin Administrators a Backup Operators mají potřebná práva k provedení ruční zálohy. Pouze členové skupiny Administrators mají potřebná práva k provedení naplánované zálohy a tato práva nelze delegovat.

Potřeba záloh

Hlavní metodou zálohování služby AD DS je replikace na druhý řadič domény. Pokud jeden řadič domény v doméně selže, další řadiče domény mají stejné informace, které zpřístupní klientům pro přihlášení a další dotazy. Za tímto účelem by v doméně měly vždy existovat alespoň dva řadiče domény. Třebaže se informace o doméně replikují mezi řadiči domény, řadič domény by měl přesto být pravidelně zálohován. Obnova existujícího řadiče domény nebo služby AD DS může být potřeba v následujících situacích:

- **Aplikace jsou nakonfigurovány tak, aby používaly konkrétní řadič domény** – některé aplikace jsou nakonfigurovány tak, aby pro přístup ke službě AD DS používaly konkrétní

řadič domény. V takovém případě obnova řadiče domény zabrání potřebě překonfigurovat danou aplikaci.

- **Všechny řadiče domény určité domény jsou zničeny** – v případě větší havárie, například při požáru budovy, mohou být všechny řadiče domény zničeny. V takovém případě musí být služba AD DS obnovena ze zálohy.
- **Objekty jsou odstraněny** – pokud dojde k náhodnému odstranění objektu služby AD DS, můžete odstraněné objekty obnovit ze zálohy. V závislosti na počtu objektů to může být rychlejší, než kdyste objekty vytvářeli znovu.

Z praxe: Příprava na havárii

První kroky při zotavení po havárii je třeba učinit dlouho předtím, než k nějaké havárii vůbec dojde. Vlastně pokud jste nevytvořili dobrý plán pro případnou havárii, problém jako selhání hardwarové komponenty na řadiči domény se může změnit spíše ve skutečnou katastrofu než jen v drobnou nesnázi.

Plánování pro případ havárie zahrnuje zvážení všech součástí, které tvoří infrastrukturu běžné sítě, stejně jako určité plánování týkající se služby AD DS. Zásadní jsou zejména následující procedury:

- Vytvořte pro řadiče domény konzistentní režim zálohování a obnovení.
- Otestujte váš plán zálohování před instalací služby AD DS a po její instalaci jej pravidelně testujte.
- Otestujte změny služby AD DS v laboratorních podmínkách. Tím minimalizujete riziko, že větší změny služby AD DS, například změny schématu, způsobí problémy v reálném prostředí.
- Nainstalujte řadiče domény služby Active Directory s hardwarovou redundancí. Většinu serverů lze objednat s určitou úrovní hardwarové redundance za malé dodatečné náklady. Například server s duálními zdroji napájení, redundantními síťovými kartami a systémem pevného disku na hardwarové úrovni by měl být standardním vybavením řadičů domény.
- Ve všech sítích, kromě těch nejmenších, byste měli nainstalovat alespoň dva řadiče domény. Služba AD DS používá cyklické protokolování pro své soubory protokolů a toto výchozí nastavení není možné změnit. Toto cyklické protokolování znamená, že v případě jednoho řadiče domény byste mohli přijít o data ve službě AD DS, pokud dojde k havárii řadiče domény a vy budete muset provést obnovení ze zálohy. Dokonce i v malé firmě je nezbytných více řadičů domény. Pokud chcete, aby všichni uživatelé používali nanejvýš jeden řadič domény, můžete změnit záznamy služby DNS úpravou priority pro každý řadič domény. Druhý řadič domény poté může plnit jinou funkci a může být použit pouze jako záložní, v případě selhání prvního řadiče domény.

Frekvence zálohování

Záloha je platná pouze po dobu životnosti objektu označeného jako neplatný, která je nakonfigurována ve službě AD DS. Zálohu služby AD DS, která je starší než životnost objektu označeného jako neplatný, nelze obnovit. Ačkoliv životnost objektu označeného jako neplatný klade vysoké nároky na frekvenci zálohování, řadiče domény byste měli zálohovat častěji, než je životnost objektu označeného jako neplatný. Pokud se pokoušíte obnovit řadič domény ze zálohy, která je více než pár dnů stará, je třeba kromě problémů

souvisejících s životností objektu označeného jako neplatný zvážit mnoho dalších problémů. Jelikož obnovení služby AD DS se týká i všech informací na nepostradatelných svazcích, tyto informace budou obnoveny do předchozího stavu. Pokud byla na serveru nainstalována role Active Directory Certificate Services, žádné certifikáty, které jste vydali před provedením zálohy, nebudou zahrnuty do databáze Active Directory Certificate Services. Pokud jste aktualizovali ovladače nebo nainstalovali nějaké nové aplikace, nemusí fungovat, neboť registr byl vrácen zpět do předchozího stavu. Většina firem používá zálohovací scénář, v němž jsou alespoň některé servery zálohovány každou noc. Řadiče domény by měly být součástí nočního zálohování.

Provádění zálohy služby AD DS pomocí programu Zálohování serveru (Windows Server Backup)

Chcete-li provést zálohu služby AD DS pomocí programu Zálohování serveru (Windows Server Backup), postupujte podle následujících kroků:

1. V podokně stromu okna nástroje Správce serveru (Server Manager) rozbalte uzel Úložiště (Storage) a poté klepněte na uzel Zálohování serveru (Windows Server Backup). Program Zálohování serveru (Windows Server Backup) můžete otevřít také z nabídky Nástroje pro správu (Administrative Tools).
2. V podokně Akce (Actions) podokna s výsledky programu Zálohování serveru (Windows Server Backup) klepněte na příkaz Zálohovat jednou (Backup Once), čímž spustíte Průvodce jednorázovým zálohováním (Backup Once Wizard). Rovněž můžete zvolit naplánování pravidelné zálohy.
3. Na stránce Možnosti zálohování (Backup Options) Průvodce jednorázovým zálohováním (Backup Once Wizard) klepněte na tlačítko Další (Next).
4. Na stránce Vybrat konfiguraci zálohování (Select Backup Configuration) můžete buď provést úplnou zálohu serveru, nebo vlastní zálohu, která vám umožní vyloučit ze zálohy některé svazky. Klepněte na tlačítko Vlastní (Custom) a poté na tlačítko Další (Next).
5. Na stránce Vybrat zálohované položky (Select Backup Items) klepněte na tlačítko Další (Next). Ve výchozím nastavení budou vybrány všechny nepostradatelné svazky na řadiči domény. Viz obrázek 17.3.
6. Na stránce Zadat typ cíle (Specify Destination Type) můžete vybrat umístění souborů záloh. Můžete vybrat místní jednotku nebo vzdálenou sdílenou složku, pokud provádíte zálohu na požádání. Klepněte na tlačítko Další (Next).
7. Na stránce Vyberte cíl zálohování (Select Backup Destination) vyberte umístění, kam chcete uložit soubor zálohy, a poté klepněte na Další (Next).
8. Na stránce Zadat upřesňující možnosti (Specify Advanced Options) můžete zvolit možnost provedení zálohování kopie ze služby VSS nebo úplné zálohování služby VSS. Klepněte na tlačítko Další (Next).
9. Na stránce Potvrzení (Confirmation) klepněte na tlačítko Zálohovat (Backup).

Pro zálohování služby AD DS můžete rovněž použít nástroj příkazového řádku Wbadmin. Pomocí tohoto nástroje můžete zazálohovat a obnovit pouze data o stavu systému na řadiči domény. Pro zálohování pouze dat o stavu systému použijte následující příkaz, v němž *Pismenojednotky:* označuje jednotku, na kterou chcete uložit soubory zálohy.

```
WBAdmin Start Systemstatebackup -backuptarget:Pimenojednotky:
```

Obnovení služby AD DS

Obnovení služby AD DS může být potřeba ze dvou důvodů: prvním důvodem je, že vaše databáze je nepoužitelná – třeba kvůli selhání pevného disku na jednom z vašich řadičů domény nebo kvůli takovém poškození databáze, že ji nebude možné načíst. Druhým důvodem je vznik problému s informacemi o databázi kvůli selhání lidského faktoru. Například pokud někdo odstranil organizační jednotku obsahující několik set uživatelských a skupinových účtů, budete chtít obnovit informace, spíše než je všechny znovu zadávat.

Pokud obnovujete službu AD DS, protože databáze na jednom z vašich řadičů domény je nepoužitelná, máte dvě možnosti. První možností je službu AD DS na poškozený server vůbec neobnovovat, ale spíše vytvořit jiný řadič domény nabídnutím jinému serveru se systémem Windows Server 2008, aby se stal řadičem domény. Tímto způsobem obnovíte funkčnost řadiče domény, místo abyste obnovili službu AD DS na určitém řadiči domény. Druhou možností obnovení je opravit server, který selhal, a poté obnovit databázi služby AD DS na tomto serveru. V tomto případě provedete neautoritativní obnovení. *Neautoritativní obnovení* obnoví databázi služby AD DS na řadiči domény a poté se na tento obnovený řadič domény replikují všechny změny provedené ve službě AD DS od provedení zálohy.

Pokud obnovujete službu AD DS proto, že někdo odstranil velký počet objektů v adresáři, máte k dispozici pouze jednu možnost obnovení informací. Obnovte databázi služby AD DS na jednom z řadičů domény pomocí zálohy, která obsahuje odstraněné objekty. Poté proveďte autoritativní (tzv. vynucené) obnovení. Během autoritativního obnovení se obnovená data označí, aby se replikovala na všechny ostatní řadiče domény, čímž se přepíše informace o odstraněných objektech.

Odebrání řadičů domény ze služby AD DS pomocí nástroje Ntdsutil

Pokud zvolíte možnost obnovení funkčnosti služby AD DS vytvořením nového řadiče domény, stále potřebujete odebrat z adresáře a ze služby DNS starý řadič domény. Pokud plánujete použít název řadiče domény, který selhal, pro obnovený řadič domény, musíte před instalací služby AD DS na nový řadič domény vyčistit adresář pomocí nástroje Ntdsutil. Pokud pro nový řadič domény používáte jiný název, můžete vyčistit adresář až po instalaci.

Chcete-li vyčistit informace o řadiči domény, který selhal, ve službě AD DS, postupujte podle následujících kroků:

1. Otevřete příkazový řádek.
2. Zadejte příkaz ntdsutil a stiskněte klávesu Enter.

3. Na příkazovém řádku Ntdsutil zadejte příkaz metadata cleanup a stiskněte klávesu Enter.
4. Na příkazovém řádku Metadata Cleanup zadejte příkaz connections a stiskněte klávesu Enter. Tento příkaz se používá k připojení k aktuálnímu řadiči domény kvůli provedení změn ve službě AD DS.
5. Na příkazovém řádku Server Connections zadejte příkaz connect to server nazevserveru, kde nazevserveru je názvem dostupného řadiče domény, a stiskněte klávesu Enter. Pokud jste přihlášení pomocí účtu, který má oprávnění správce ve službě AD DS, budete připojeni k tomuto řadiči domény. Pokud nemáte práva správce, můžete použít příkaz set creds domena uzivatelske_jmeno heslo k zadání pověření uživatele s oprávněními na úrovni domény.
6. Na příkazovém řádku Server Connections zadejte příkaz quit a stiskněte klávesu Enter. Tím se vrátíte na příkazový řádek příkazu Metadata Cleanup.
7. Na příkazovém řádku Metadata Cleanup zadejte příkaz select operation target a stiskněte klávesu Enter. Tento příkaz se používá k výběru domény, lokality a řadiče domény, abyste mohli odebrat řadič domény.
8. Na příkazovém řádku Select Operations Target zadejte příkaz list domains a stiskněte klávesu Enter. Všechny domény v doménové struktuře se vypíší s přiřazenými čísly.
9. Na příkazovém řádku Select Operations Target zadejte příkaz select domain cislo, kde cislo označuje doménu obsahující řadič domény, který selhal, a stiskněte klávesu Enter.
10. Na příkazovém řádku Select Operations Target zadejte příkaz list sites a stiskněte klávesu Enter. Všechny lokality v doménové struktuře se vypíší s přiřazenými čísly.
11. Na příkazovém řádku Select Operations Target zadejte příkaz select site cislo, kde cislo označuje lokalitu obsahující řadič domény, který selhal, a stiskněte klávesu Enter.
12. Na příkazovém řádku Select Operations Target zadejte seznam list servers in site a stiskněte klávesu Enter.
13. Na příkazovém řádku Select Operations Target zadejte příkaz select server cislo, kde cislo označuje řadič domény, který selhal, a stiskněte klávesu Enter.
14. Zadejte příkaz quit a stiskněte klávesu Enter. Tím se vrátíte do příkazového řádku příkazu Metadata Cleanup.
15. Zadejte příkaz remove selected server a stiskněte klávesu Enter.
16. Klepnutím na tlačítko Ano (Yes) potvrďte odebrání serveru.
17. Zadáním příkazu quit na každém příkazovém řádku ukončete nástroj Ntdsutil.

Poznámka: Tento proces pomocí nástroje Ntdsutil se rovněž používá tehdy, když jste vynutili odebrání služby AD DS ze serveru pomocí příkazu *Dcpromo /forceremoval*. Tento příkaz sníží úroveň řadiče domény bez vyčištění metadat ve službě AD DS. Pokud bude služba AD DS z nějakého důvodu nepoužitelná, tento příkaz může být alternativou ke kompletnímu obnovení serveru.

Kromě vyčištění objektu adresáře pomocí nástroje Ntdsutil byste měli vyčistit záznamy DNS pro řadič domény, který selhal. Odstraňte všechny DNS záznamy ze služby DNS, včetně všech záznamů řadiče domény, záznamů serveru globálního katalogu a záznamů emulátoru primárního řadiče domény. (Poslední dva typy záznamů budou existovat pouze v případě, že řadič domény byl nakonfigurován s těmito rolemi.) Pokud nevyčistíte záznamy DNS, klienti budou nadále přijímat informace DNS a budou se pokoušet připojit k řadiči domény. To může vést k pomalejším připojením ke službě AD DS, neboť klienti při selhání použijí náhradní řadiče domény.

Provádění neautoritativního obnovení služby AD DS

Neautoritativní obnovení služby AD DS se provádí ve dvou situacích. Když dojde k poškození databáze služby AD DS na serveru, provedení neautoritativního obnovení služby AD DS znovu vytvoří databázi a umožní její fungování. Pokud provedete úplné obnovení řadiče domény, rovněž použijte neautoritativního obnovení služby AD DS. Úplné obnovení řadiče domény je vyžadováno v případě, že jediný řadič domény v dané doméně selže. Úplné obnovení řadiče domény můžete provést také tehdy, pokud chcete, aby identita řadiče domény, který selhal, zůstala stejná.

Pokud jste od poslední zálohy provedli libovolné změny služby AD DS, zálohovací páska nebude tyto změny obsahovat. Ovšem jiné řadiče domény v dané doméně budou mít nejaktuálnější informace. Pokud znovu vytváříte řadič domény kvůli selhání serveru, tento řadič domény by měl získat změny od svých partnerů pro replikaci po dokončení obnovení.

Chcete-li provést neautoritativní obnovení služby AD DS, restartujte počítač a spusťte jej v Režimu obnovení adresářových služeb (Directory Services Restore Mode) (DSRM), obnovte stav systému z nepostradatelných svazků pomocí nástroje Wbadmin.exe a poté běžně restartujte systém Windows Server 2008. Když se řadič domény restartuje, připojí se ke svým partnerům pro replikaci a začne aktualizovat svou vlastní databázi tak, aby reflektovala všechny informace o doméně, které se od poslední zálohy změnily.

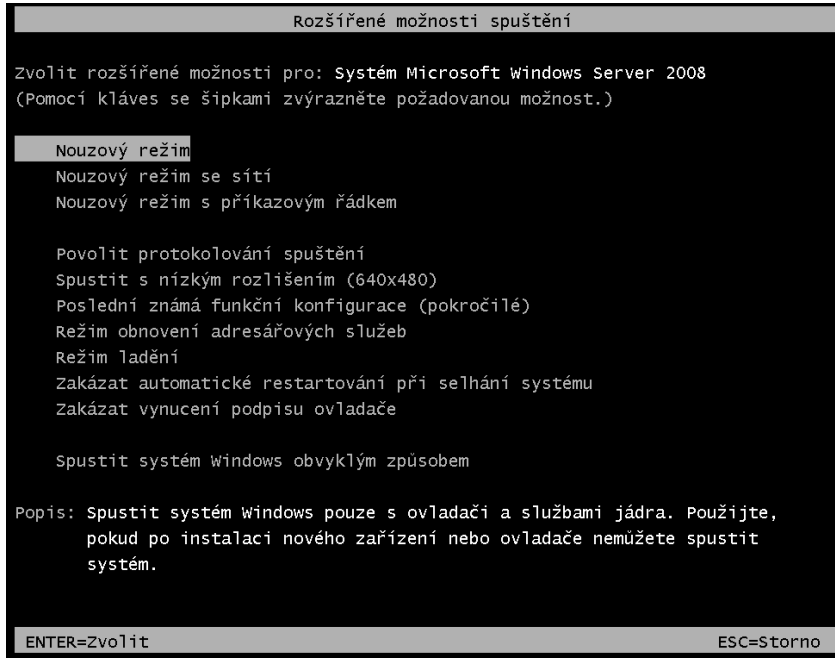
DSRM je verzí nouzového režimu pro řadiče domény, v němž je služba AD DS zastavena. Chcete-li se přihlásit do režimu DSRM, musíte použít účet správce pro režim DSRM, který je vytvořen při instalaci služby AD DS. Jedná se o místní účet správce vytvořený během instalace služby AD DS na řadiči domény. Heslo je nastaveno při instalaci a není stejné jako heslo správce domény.

Poznámka: V systémech Windows Server 2003 a Windows Server 2008 se nástroj Ntdsutil používá k vytvoření nového hesla k účtu správce pro režim DSRM. V kontextu příkazu Set Dsrm Password použijte příkaz *reset password of server server*, kde *server* je názvem řadiče domény, na kterém chcete vytvořit nové heslo k účtu správce pro režim DSRM. Pokud chcete specifikovat místní server, můžete pro server použít hodnotu *null*.

Chcete-li provést neautoritativní obnovení služby AD DS, postupujte podle následujících kroků:

1. Opravte řadič domény, který selhal. V tuto chvíli bude server funkční s výjimkou služby AD DS.

2. Restartujte server a stisknutím klávesy F8 otevřete nabídku Rozšířené možnosti spuštění (Advanced Boot Options). Viz obrázek 17.4.



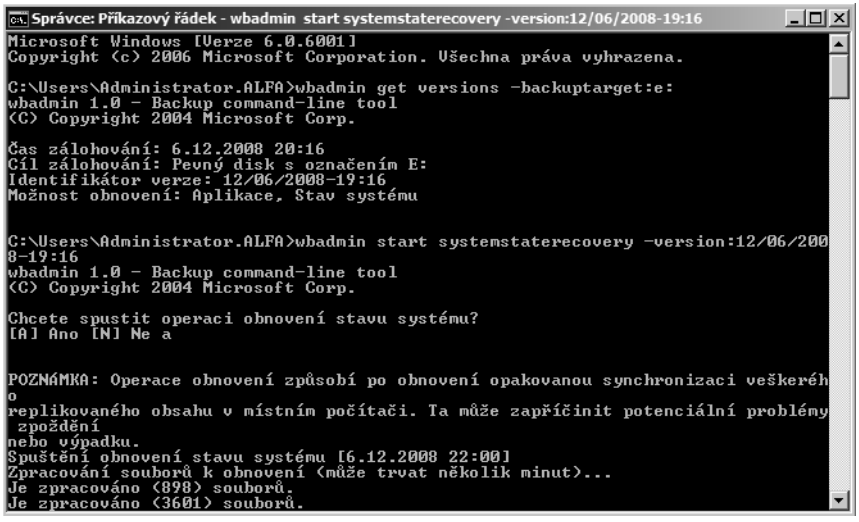
Obrázek 17.4: Nabídka Rozšířené možnosti spuštění (Advanced Boot Options) s režimem DSRM

3. Zvolte možnost Režim obnovení adresářových služeb (Directory Services Restore Mode).

Poznámka: Alternativou k použití nabídky Rozšířené možnosti spuštění (Advanced Boot Options) je příkaz *bcdedit /set safeboot dsrepair*, pomocí něhož můžete jako výchozí možnost spouštění nastavit režim Directory Services Restore Mode (DSRM). Po dokončení instalace použijte příkaz *bcdedit /deletevalue safeboot* a restartováním serveru spusťte systém Windows obvyklým způsobem.

4. Přihlašte se pomocí účtu správce pro režim DSRM. Abyste se přihlásili jako tento uživatel, zadejte jako uživatelské jméno hodnotu .\Administrator.
5. Otevřete příkazový řádek.
6. Zadejte příkaz wbadmin get versions –backuptarget:umistenizalohy, kde umistenizalohy je písmeno jednotky nebo cesta UNC k uložené záloze, a stiskněte klávesu Enter. Tím vypíšete seznam záloh uložených v zadaném umístění.
7. Všimněte si identifikátoru verze zálohy, kterou si přejete obnovit. Tento identifikátor je časem, kdy byla záloha vytvořena.

8. Zadejte příkaz wbadmin start systemstaterecovery –version:identifikator –backuptarget:umistenizalohy, kde identifikator je identifikátorem verze zmíněným v kroku 7 a umistenizalohy je písmeno jednotky nebo cesta UNC k uložené záloze, a stiskněte klávesu Enter. Obrázek 17.5 znázorňuje obnovení stavu systému pomocí nástroje Wbadmin.



Obrázek 17.5: Obnovení stavu systému pomocí nástroje Wbadmin.exe

9. Zadejte A (Y) a stisknutím klávesy Enter zahajte obnovu stavu systému.

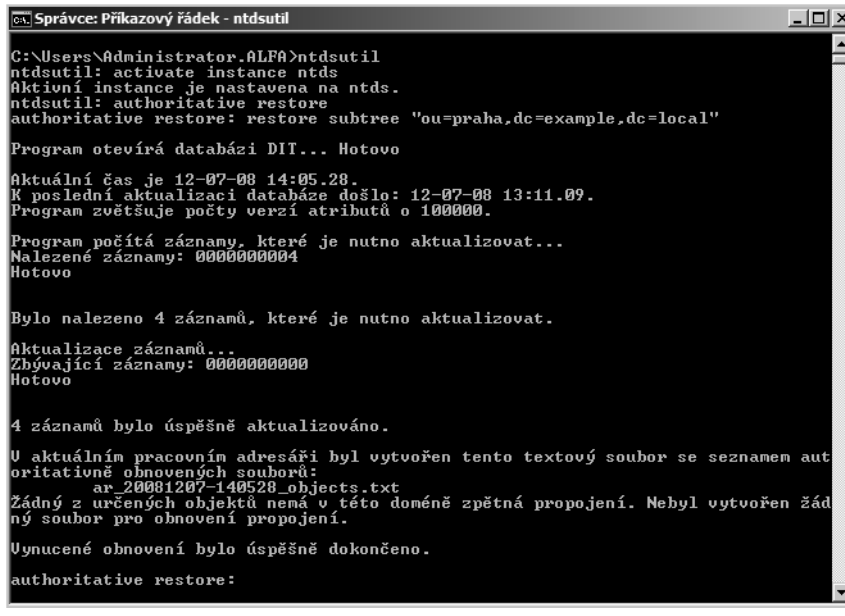
10. Po dokončení obnovení restartujte řadič domény.

Provádění autoritativního obnovení služby AD DS

Autoritativní obnovení je vyžadováno v situacích, kdy potřebujete obnovit objekty, které byly odstraněny ze služby AD DS. Například pokud někdo pouze odstranil organizační jednotku, která obsahuje několik set uživatelů, nebudete chtít, aby se řadič domény jednoduše restartoval po provedení obnovení a poté zahájil replikaci s ostatními řadiči domény. Pokud byste tak učinili, řadič domény obdrží od svých partnerů pro replikaci informaci o tom, že organizační jednotka byla odstraněna, a než otevřete nástroj pro správu Uživatelé a počítače služby Active Directory (Active Directory Users And Computers), organizační jednotka se opět odstraní.

V takovém scénáři musíte použít autoritativní obnovení, abyste zajistili, že obnovení organizační jednotky bude replikováno na ostatní řadiče domény. Po provedení autoritativního obnovení obnovte záložní kopii služby AD DS, která byla vytvořena před odstraněním dat, a poté vynuťte replikaci těchto dat na všechny ostatní řadiče domény. Vynucení replikace dosáhnete zpracováním pořadového čísla aktualizací (USN) pro obnovené informace. Ve výchozím nastavení platí, že při autoritativním obnovení se pořadové číslo aktualizací zvýší o 100 000, aby se obnovené objekty staly autoritativní kopií pro celou doménu.

Základní proces provedení autoritativního obnovení služby AD DS je stejný jako neautoritativní obnovení – až na jeden krok. Po dokončení obnovení služby AD DS v režimu DSRM použijte nástroj Ntdsutil ke specifikování, které objekty jsou autoritativní, viz obrázek 17.6. Můžete specifikovat samotné objekty nebo podstrom v doméně.



Obrázek 17.6: Použití nástroje Ntdsutil ke specifikaci autoritativních objektů po obnovení

Chcete-li provést autoritativní obnovení, postupujte podle následujících kroků:

1. Restartujte server a stisknutím klávesy F8 vstupte do nabídky Rozšířené možnosti spuštění (Advanced Boot Options).
2. Zvolte možnost Režim obnovení adresářových služeb (Directory Service Restore Mode).
3. Přihlaste se pomocí účtu správce pro režim DSRM. Abyste se přihlásili jako tento uživatel, zadejte jako uživatelské jméno hodnotu .\Administrator.
4. Otevřete příkazový řádek.
5. Zadejte příkaz wbadmin get versions –backuptarget:umistenizalohy, kde umistenizalohy je písmeno jednotky nebo cesta UNC k uložené záloze, a stiskněte klávesu Enter. Tím vypíšete seznam záloh uložených v zadaném umístění.
6. Všimněte si identifikátoru verze zálohy, kterou si přejete obnovit. Tento identifikátor je časem, kdy byla záloha vytvořena.
7. Zadejte příkaz wbadmin start systemstaterecovery –version:identifikator –backuptarget:umistenizalohy, kde identifikator je identifikátorem verze zmíněným v kroku 7 a umistenizalohy je písmeno jednotky nebo cesta UNC k uložené záloze, a stiskněte klávesu Enter. Obrázek 17.5 znázorňuje obnovení stavu systému pomocí nástroje Wbadmin.

8. Zadejte A (Y) a stisknutím klávesy Enter zahajte obnovu stavu systému.
9. Po dokončení obnovení zadejte příkaz ntdsutil a stiskněte klávesu Enter..
10. Na příkazovém řádku Ntdsutil zadejte příkaz activate instance ntds a stiskněte klávesu Enter.
11. Na příkazovém řádku Ntdsutil zadejte příkaz authoritative restore a stiskněte klávesu Enter.
12. Chcete-li obnovit jeden objekt: na příkazovém řádku Authoritative Restore zadejte příkaz restore object "DN", kde DN je rozlišující název objektu, který má být autoritativně obnoven. Proces obnovení specifikuje umístění souboru LDIF pro obnovení objektů se zpětnou vazbou, pokud jsou nějaké obnoveny.
13. Chcete-li obnovit hierarchii organizačních jednotek: na příkazovém řádku Authoritative Restore zadejte příkaz restore subtree "DN", kde DN je rozlišující název organizační jednotky, v níž začíná hierarchii, která má být autoritativně obnovena. Proces obnovení specifikuje umístění souboru LDIF pro obnovení objektů se zpětnou vazbou, pokud jsou nějaké obnoveny.
14. Ukončete nástroj Ntdsutil a restartujte server.

Správa schématu služby AD DS

Schéma představuje plán služby AD DS diktující, jaké druhy objektů mohou v databázi existovat a jaké jsou atributy těchto objektů. Chcete-li přizpůsobit službu AD DS pro použití v síti, můžete změnit schéma, abyste mohli vytvářet nové typy objektů, přidávat do existujících typů objektů nové atributy a měnit typ informací v atributu. K tomu použijte modul snap-in konzoly MMC s názvem Schéma služby Active Directory (Active Directory Schema).

Změna schématu je úlohou, kterou průměrný správce nebude muset nikdy provádět. Schéma změníte nanejvýš příležitostně nebo možná pouze jednou. Pro změnu schématu platí stejná upozornění jako pro změnu registru systému Windows Server 2008, jen ve větším měřítku. Stejně jako nesprávné změny registru mohou nepříznivě ovlivnit jeden systém, nesprávné změny schématu mohou mít devastující následky na celou síť.

Z praxe: Provádění změn schématu

Dva nejčastější scénáře pro změnu schématu služby AD DS jsou situace, kdy aktualizujete doménovou strukturu z dřívější verze služby Active Directory na novější verzi a při instalaci aplikací povolených v adresáři. Novější verze služby Active Directory vždy obsahují nové funkce a mnoho z těchto funkcí vyžaduje nové objekty nebo atributy ve službě AD DS. To znamená, že prvním krokem při aktualizaci doménové struktury služby Active Directory systému Windows Server 2003 na službu AD DS systému Windows Server 2008 je spuštění buď nástroje Adprep, nebo Forestprep. Tyto nástroje provádí změny schématu vyžadované při instalaci řadičů domény systému Windows Server 2008

Druhým častým scénářem pro změnu schématu služby AD DS je situace, kdy instalujete aplikace povolené v adresáři, například Exchange Server 2007. Exchange Server 2007 vyžaduje několik stovek nových objektů ve službě AD DS, takže musíte před instalací

Exchange Serveru rozšířit schéma. Pro přípravu doménové struktury služby AD DS na Exchange Server 2007 musíte spustit instalační program Exchange Serveru s parametrem */prepareAD*.

V obou těchto případech jsou změny schématu služby AD DS zahrnuty do souborů .ldf. Během procesu aktualizace schématu se tyto soubory importují do schématu služby AD DS pomocí nástroje LDIFDE. Nejvhodnější by bylo emulovat tento proces při vytváření změn schématu. Místo ruční úpravy schématu vytvořte a důkladně otestujte soubor .ldf, který obsahuje vaše změny schématu. Poté pomocí nástroje LDFIDE importujte soubor .ldf do služby AD DS.

Požadavky na změnu schématu služby AD DS

Jelikož změna schématu služby AD DS není něco, co byste dělali bezmyšlenkovitě, schéma můžete změnit pouze na jednom řadiči domény v dané doménové struktuře a učinit tak můžete pouze tehdy, pokud je váš uživatelský účet členem skupiny Schema Admins.

Kvůli důležitosti schématu v prostředí služby AD DS mohou být změny schématu prováděny pouze na jednom řadiči domény v dané doménové struktuře. Tento řadič domény je hlavním operačním serverem schématu (Schema Operations Master). Ve výchozím nastavení je hlavním operačním serverem schématu první řadič domény nainstalovaný v dané doménové struktuře. Pro provedení změn schématu musíte být přihlášeni k hlavnímu operačnímu serveru schématu nebo musíte být přihlášení k serveru nebo pracovní stanici v doméně se systémem Windows Server 2008 pomocí účtu, který je členem skupiny Schema Admins.

Jedná se o předdefinovanou skupinu vytvořenou při instalaci služby AD DS, která uděluje svým členům oprávnění k zápisu do objektu schématu. Účet správce v kořenové doméně dané doménové struktury je automaticky členem skupiny Schema Administrators, ovšem členové skupiny Domain Admins nejsou automaticky členy skupiny Schema Admins. Uživatelé, kteří nejsou členy této skupiny, mohou rovněž měnit schéma, pokud jim správce udělil potřebná oprávnění k objektu schématu.

Důležité: Je velmi důležité, abyste striktně omezili členy skupiny Schema Admins. Nepřidávejte do této skupiny nové správce automaticky a nepřihlašujte se stále pomocí účtu, který je členem skupiny Schema Admins.

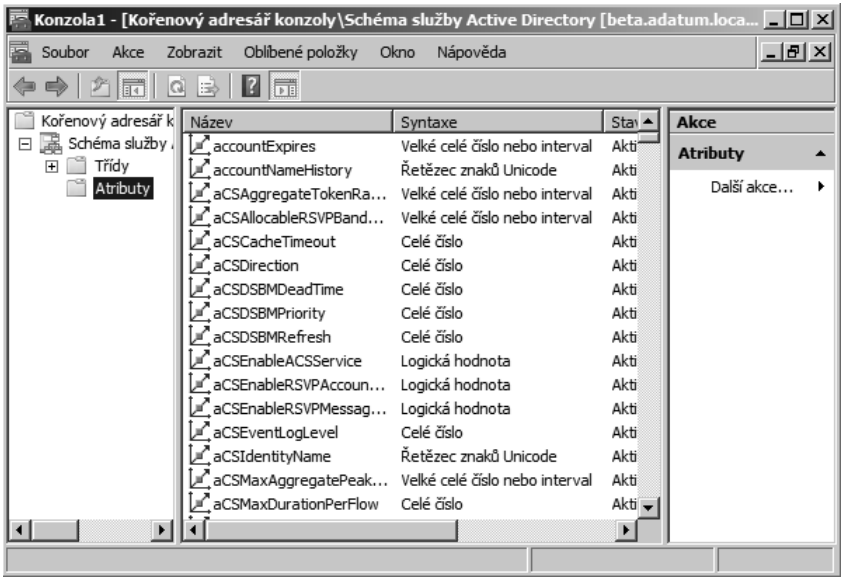
Spuštění schématu služby Active Directory

Kvůli svému příležitostnému použití a potenciálnímu nebezpečí není modul snap-in Active Directory Schema ve výchozím nastavení přidán do nabídky Administrative Tools na řadiči domény. Pokud chcete tento modul snap-in použít, musíte nejprve zaregistrovat knihovnu schmgmt.dll a poté přidat modul snap-in do konzoly MMC. Chcete-li spustit modul snap-in Active Directory Schema, postupujte podle následujících kroků:

1. Abyste zaregistrovali knihovnu dll, otevřete příkazový řádek, zadejte příkaz Regsvr32 schmmgmt.dll a poté stiskněte klávesu Enter.
2. Chcete-li přidat modul snap-in Schéma služby Active Directory (Active Directory Schema) do konzoly MMC, klepněte na tlačítko Start a zvolte příkaz Spustit (Run). Zadejte příkaz mmc a stiskněte klávesu Enter.

3. V nabídce Soubor (File) prázdné konzoly MMC klepněte na příkaz Přidat nebo odebrat modul snap-in (Add/Remove Snap-In).

4. V seznamu modulů snap-in, které jsou k dispozici, klepněte na modul snap-in Schéma služby Active Directory (Active Directory Schema), klepněte na tlačítko Přidat (Add) a poté klepněte na tlačítko OK. Po načtení modulu snap-in můžete obrazovku konzoly uložit do souboru a usnadnit si tak v budoucnu přístup k tomuto modulu snap-in. Po otevření podokna zobrazení uvidíte ve stromu konzoly dva kontejnery, které obsahují objekty tříd a atributy, které tvoří tyto třídy, viz obrázek 17.7. Výběrem některého z těchto kontejnerů zobrazíte třídy nebo atributy služby AD DS v podokně výsledků.



Obrázek 17.7: Objekty tříd a atributů modulu snap-in správce schématu uložené ve službě AD DS

Před změnou schématu se přesvědčte, že modul snap-in Schéma služby Active Directory (Active Directory Schema) je připojen k řadiči domény, který aktuálně slouží jako hlavní operační server schémat (tj. jeden řadič domény, ke kterému je povolen přístup pro zápis do schématu). Chcete-li se připojit k hlavnímu operačnímu serveru schématu, klepněte pravým tlačítkem myši na objektu Schéma služby Active Directory (Active Directory Schema) ve stromu konzoly a v místní nabídce klepněte na příkaz Připojit k hlavnímu operačnímu serveru schématu (Connect To Schema Operations Master).

Změna schématu

Proces změny schématu služby AD DS zahrnuje vytvoření nebo změnu typů objektů tříd a atributů zobrazených v modulu snap-in Schéma služby Active Directory (Active Directory Schema). *Třídy* jsou v podstatě kolekce atributů, které buď tvoří typ objektu služby AD DS samy o sobě, nebo přispívají určitými atributy k jinému typu objektu. Druhý případ je znám jako *pomocná třída*. Chcete-li přidat atributy k existujícímu typu objektu, nejlepším způsobem je vytvořit novou třídu obsahující nové atributy a přidat ji

k typu objektu jako pomocnou. Tento způsob umožňuje lepší správu a je méně nebezpečný než změna samotné třídy reprezentující typ objektu.

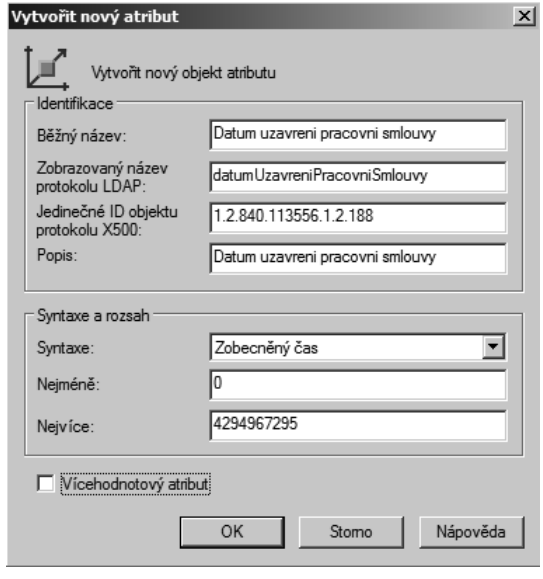
Softwarové produkty od jiných výrobců by mohly podporovat vlastní změny schématu, které vytváří zcela nové typy objektů, ale přidání atributů k existujícímu typu objektu je nejčastější formou změny schématu ručně prováděnou správci – například přidání atributů k uživatelskému typu objektu, který vám umožňuje uložení dalších informací o uživateli ve službě AD DS. Tento relativně snadný proces sestává z následujících kroků, které jsou podrobněji popsány v dalších částech:

- Vytvoření nových objektů atributů odpovídajících informačním polím, která chcete přidat do objektu.
- Přidání nově vytvořených atributů do nové pomocné třídy.
- Přidání pomocné třídy do existující třídy objektů.

Vytváření atributů

Vytvoření atributu spočívá v zadání názvu, pod kterým bude daný atribut identifikován, a v zadání typu dat, která v něm budou uložena. Data může tvořit text nebo číslo a můžete použít omezení, která omezí data na určitou délku nebo typ hodnoty. Například pro přidání atributu, který má obsahovat datum přijetí zaměstnance, určete, že data atributu mohou být zadána jako zobecněný čas. Chcete-li vytvořit objekt atributu, postupujte podle následujících kroků:

1. Klepněte pravým tlačítkem myši na kontejneru Atributy (Attributes) ve stromu konzoly Schéma služby Active Directory (Active Directory Schema) a v místní nabídce klepněte na příkaz Vytvořit atribut (Create Attribute). Nejprve se zobrazí upozornění, že vytvoření objektu trvale změní službu AD DS a poté se zobrazí dialog Vytvořit nový atribut (Create New Attribute), znázorněný na obrázku 17.8.



Obrázek 17.8: Dialog Vytvořit nový atribut (Create New Attribute)

2. V části Identifikace (Identification) zadejte název nového objektu. Pole Běžný název (Common Name) by mělo obsahovat název, pod kterým bude atribut zobrazen v běžných dialozích, a pole Zobrazovaný název protokolu LDAP (LDAP Display Name) by mělo obsahovat název, pod kterým bude znám v hierarchii adresáře LDAP. (LDAP je zkratkou z ang. Lightweight Directory Access Protocol.) Často jsou tyto dva názvy stejné. Pole Jedinečné ID objektu protokolu X.500 (Unique X.500 Object ID) musí obsahovat číselný řetězec, který jednoznačně identifikuje objekt atributu v jmenném prostoru protokolu X.500. Standardizační organizace, jako je International Telecommunications Union, vydává identifikátory objektů (OID) k zajištění jejich jedinečných hodnot. Do pole Popis (Description) zadejte popis objektu a jeho funkci.

Další informace: Identifikátory objektů můžete získat buď přímo od registrační autority ISO Name Registration, nebo od společnosti Microsoft. Pokud hodláte rozšířit schéma služby AD DS a chcete zažádat o logo Certified For Windows, musíte si zaregistrovat identifikátor objektu u společnosti Microsoft. Další informace o získání identifikátoru objektu od registrační autority ISO najdete na adrese *http://msdn2.microsoft.com/en-us/library/ms677621.aspx*. Chcete-li získat základní identifikátor objektu přímo od společnosti Microsoft, informace hledejte na adrese *http://msdn2.microsoft.com/en-us/library/ms677620(VS.85).aspx*.

3. V části Syntaxe a rozsah (Syntax And Range) definujte povahu dat, která mají být v atributu uložena. Pole Syntaxe (Syntax) nabízí více než tucet možností, které definují typy informací, které mohou být v daném atributu uloženy. Pole Nejméně (Minimum) a Nejvíce (Maximum) vám umožní definovat rozsah možných hodnot. Rovněž můžete specifikovat, zda by měl atribut být schopen nabývat více hodnot.
4. Po klepnutí na tlačítko OK se vytvoří nový objekt atributu.

Nový (nebo kterýkoliv jiný) objekt atributu můžete rovněž nakonfigurovat otevřením dialogu Vlastnosti (Properties) z místní nabídky, viz obrázek 17.9. V tomto okně můžete zadat popis objektu, změnit jeho rozsah možných hodnot a povolit další následující možnosti:

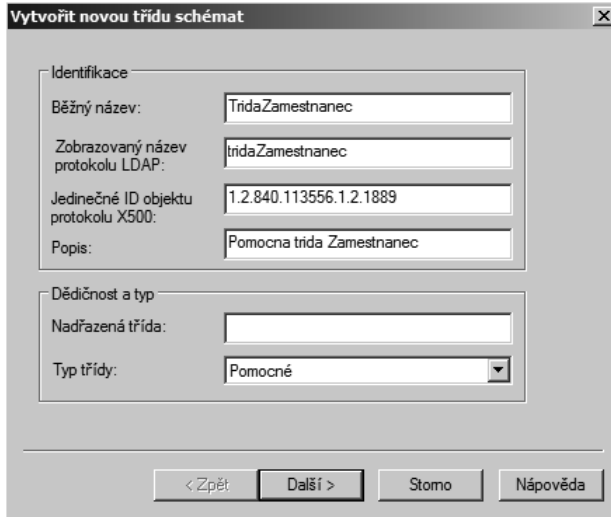
- deaktivovat tento atribut
- zařadit tento atribut do indexu služby Active Directory
- překládat dvojjazyčné názvy (ANR)
- replikovat tento atribut do globálního katalogu (GC)
- při duplikaci uživatele zkopírovat atribut
- zařadit tento atribut do indexu pro kontejnerizovaná vyhledávání

Důležité: Třebaže můžete deaktivovat změny, které ve schématu provedete, nikdy nemůžete odstranit nové třídy nebo atributy, které ve schématu vytvoříte. Změny ve schématu byste měli provádět teprve po pečlivém naplánování a důkladném testování v testovací doménové struktuře. Přesvědčte se, že změny vašeho schématu jsou kompatibilní s aktuálními a budoucími aplikacemi, které vyžadují změny schématu.

Obrázek 17.9: Dialog Vlastnosti (Properties) objektu atributu

Vytváření tříd objektů

Objekty atributů jsou samy o sobě neužitečné, dokud nepatří do nějaké třídy objektu. Objekty atributu, které vytvoříte, můžete přidat k existující třídě, ale vytvoření nové třídy objektu pro tyto objekty je obecně praktičtější. Chcete-li vytvořit objekt třídy, klepněte pravým tlačítkem myši na kontejneru Třídy (Classes) v modulu snap-in Schéma služby



Obrázek 17.10: Dialog Vytvořit novou třídu schématu (Create New Schema Class)

Active Directory (Active Directory Schema) a v místní nabídce zvolte příkaz Vytvořit třídu (Create Class). Tím zobrazíte dialog Vytvořit novou třídu schématu (Create New Schema Class), znázorněný na obrázku 17.10.

Stejně jako v případě objektu atributu musíte nejprve vyplnit pole Běžný název (Common Name), Zobrazovaný název protokolu LDAP (LDAP Display Name) a Jedinečné ID objektu protokolu X.500 (Unique X.500 Object ID). Poté v části Dědičnost a typ (Inheritance And Type) vyplňte pole Nadřazená třída (Parent Class) pro nový objekt (tedy třídu, od níž má být nový objekt odvozen) a vyberte jeden z následujících tří typů tříd:

- **Konstrukční třída (Structural)** – typické objekty adresáře, s nimiž pracujete v programech jako Uživatelé a počítače služby Active Directory (Active Directory Users And Computers). Nadřazeným objektem objektu konstrukční třídy může být buď abstraktní třída, nebo jiná konstrukční třída.
- **Abstraktní třída (Abstract)** – objekty, z nichž jsou odvozeny objekty konstrukční třídy. Jako nadřazený objekt nového objektu abstraktní třídy můžete určit také existující abstraktní třídu.
- **Pomocná třída (Auxiliary)** – kolekce atributů, které můžete přidat buď do abstraktní, nebo konstrukční třídy objektu, abyste rozšířili její možnosti. Nové objekty pomocné třídy mohou být odvozeny pouze od abstraktních tříd.

Chcete-li zachovat své nové atributy, vytvořte typ pomocné třídy.

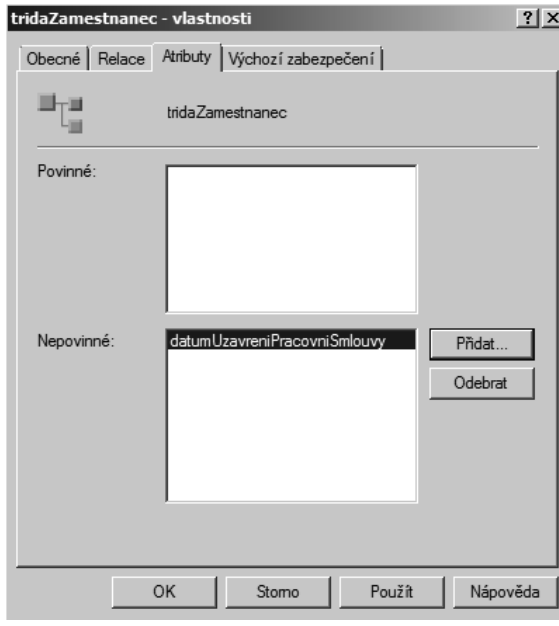
Přidání atributů do třídy

Po vytvoření objektů atributu a objektu třídy, který je má obsahovat, musíte přidat atributy do třídy. To provedete otevřením dialogu Vlastnosti (Properties) s vlastnostmi nově vytvořeného objektu třídy. Tento dialog pro objekt třídy obsahuje čtyři karty, včetně karty Výchozí zabezpečení (Default Security). Na kartě Obecné (General) zadejte popis objektu a určete, zda se má objekt třídy zobrazovat při vyhledávání. Rovněž můžete zakázat objekt zrušením zaškrtnutí políčka Třída je aktivní (Class Is Active).

Na kartě Atributy (Attributes) (znázorněné na obrázku 17.11) přidejte nově vytvořené objekty atributů do třídy klepnutím na tlačítko Přidat (Add) buď u seznamu Povinné (Mandatory), nebo Nepovinné (Optional) a poté výběrem objektů podle jejich názvu. Pokud je atribut povinný, musíte zadat hodnotu atributu při vytváření nového objektu dané třídy. Pokud například vytváříte atribut *DatumUzavreniPracovniSmlouvy*, přidejte jej do vaší pomocné třídy jako povinný atribut a poté přidejte povinnou třídu do uživatelské třídy; při dalším vytvoření nového uživatelského objektu bude pro uživatele požadováno zadání atributu Cislo zamestnance. Hodnoty volitelných atributů nejsou vyžadovány.

Přidání pomocné třídy ke konstrukční třídě

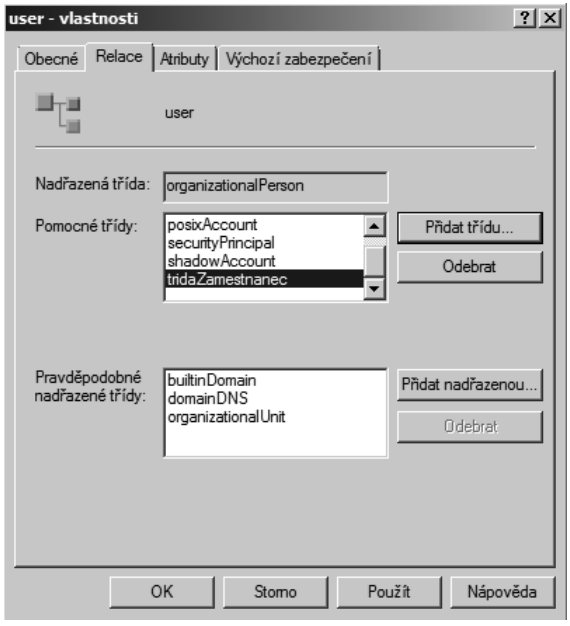
Objekt pomocné třídy nemůže uchovávat informace o atributech, dokud nepřidáte objekt pomocné třídy do objektu konstrukční třídy, jako je například uživatel nebo počítač. To provedete otevřením dialogu Vlastnosti (Properties) daného objektu konstrukční třídy a výběrem karty Relace (Relationship), znázorněné na obrázku 17.12.



Obrázek 17.11: Karta Atributy (Attributes) dialogu Vlastnosti (Properties)

Na této kartě klepněte na tlačítko Přidat třídu (Add Class) u seznamu Pomocné třídy (Auxiliary Classes) a vyberte objekt třídy, který jste právě vytvořili. Služba AD DS tak přidá atributy v pomocné třídě do konstrukční třídy. V seznamu Pravděpodobně nadřazené třídy (Possible Superior) určete, které další třídy objektů mohou obsahovat aktuální třídu objektů. Například třída uživatelských objektů obsahuje třídu objektů organizační jednotky ve svém seznamu Pravděpodobně nadřazené třídy (Possible Superior), který umožňuje vytvoření nových uživatelů v dané organizační jednotce. Naopak to však neplatí: pod uživatelem nemůžete vytvořit organizační jednotku, takže uživatelský objekt není na seznamu možných nadřazených tříd objektu organizační jednotky.

Poznámka: Přidání nového atributu do schématu neznamená, že tento atribut bude automaticky přístupný z libovolného nástroje pro správu. Nástroje pro správu, například Uživatelé a počítače služby Active Directory (Active Directory Users And Computers), zobrazují pouze některé atributy každé třídy a nezobrazují všechny atributy, které přidáte. Pokud chcete, aby se nový atribut objevil v nástroji pro správu, musíte buď změnit existující nástroj, nebo si vytvořit vlastní nástroj. Další informace o změně a vytváření nástrojů pro správu najdete v článku „Extending the User Interface for Directory Objects" na adrese *http://msdn2.microsoft.com/en-us/library/ms676902.aspx*. Nástroj Editor ADSI (ADSI Edit) zobrazí nové atributy, protože seznam dostupných atributů objektu se dynamicky načítá ze schématu.



Obrázek 17.12: Karta Relace (Relationship) dialogu Vlastnosti (Properties)

Správa rolí hlavních operačních serverů

Služba AD DS je navržena jako systém replikace multimaster. Ten vyžaduje, aby všechny řadiče domény jiné než řadiče domény jen pro čtení měly oprávnění zapisovat do databáze adresáře. Tento systém funguje dobře pro většinu operací adresáře, ale pro určité operace adresáře je vyžadován jediný autoritativní server. Řadiče domény, které plní konkrétní role, jsou známé jako *hlavní operační servery* a každý z nich plní roli FSMO (flexible single-master operations). Řadiče domény, které plní role hlavního operačního serveru, jsou určeny k provádění konkrétních úloh zajišťujících konzistenci a eliminujících možnosti konfliktních položek v databázi služby AD DS. Služba AD DS obsahuje následujících pět rolí hlavního operačního serveru:

- hlavní server schémat (Schema master),
- hlavní operační server pro pojmenování domén (Domain naming master),
- hlavní server RID (RID master),
- emulátor primárního řadiče domény (PDC emulator),
- hlavní server infrastruktury (Infrastructure master).

První dvě role, hlavní server schémat a hlavní operační server pro pojmenování domén, jsou role pro doménovou strukturu. To znamená, že pro každou doménovou strukturu existuje pouze jeden hlavní server schémat a pouze jeden hlavní operační server pro pojmenování domén. Zbývající tři role jsou role pro doménu – pro každou doménu v doménové struktuře existuje jedna z těchto rolí hlavních operačních serverů. Po nainstalování služby AD DS a vytvoření prvního řadiče domény v doménové struktuře bude

plnit všech těchto pět rolí. Podobně, jakmile přidáte domény do doménové struktury, první řadič domény v každé nové doméně rovněž obdrží role hlavního operačního serveru pro danou doménu. Jakmile do domény přidáte nové řadiče domény, můžete tyto role přenést na jiné řadiče domény.

Hlavní server schémat

Jak bylo již popsáno výše, hlavní server schémat je jediným řadičem domény, který má oprávnění k zápisu do schématu adresáře. K provádění jakýchkoliv změn schématu musí být správce (který musí být členem skupiny zabezpečení Schema Admins) připojen k hlavnímu serveru schémat. Pokud se pokusíte o změnu schématu na řadiči domény jiném než na hlavním serveru schématu, tento pokus bude neúspěšný. Po provedení změny se aktualizace schématu replikují na všechny ostatní řadiče domény v doménové struktuře.

Hlavní názvový operační server pro pojmenování domén

Hlavní operační server pro pojmenování domén je řadičem domény, který spravuje přidávání a odebírání všech součástí adresáře v hierarchii doménové struktury. Řadič domény, který plní roli hlavního operačního serveru pro pojmenování domén, musí být dostupný při následujících operacích:

- **Přidání nebo odebrání domény** – při vytváření nebo odebrání podřízené domény nebo nového stromu domény instalační průvodce kontaktuje hlavní operační server pro pojmenování domén a požádá o přidání nebo odstranění. Hlavní operační server pro pojmenování domén je zodpovědný za zajištění jedinečnosti názvů domén. Pokud je hlavní operační server pro pojmenování domén nedostupný, nemůžete přidávat domény z doménové struktury ani je z ní odebírat.
- **Přidání nebo odebrání oddílů adresáře aplikace** – oddíly adresáře aplikace jsou speciální oddíly, které mohou být vytvořeny na řadičích domény se systémem Windows Server 2003 nebo Windows Server 2008 a které nabízí úložiště pro data dynamických aplikací. Pokud je řadič domény, který je hostitelem role hlavního operačního serveru pro pojmenování domén, nedostupný, nemůžete přidat ani odebrat oddíly adresáře aplikace z doménové struktury.
- **Přidání nebo odebrání objektů křížového odkazu** – po vytvoření nové doménové struktury se na prvním řadiči domény v doménové struktuře vytvoří schéma, konfigurace a oddíly adresáře domény. Objekt křížového odkazu se vytvoří pro každý oddíl adresáře v kontejneru Partitions v oddílu konfigurace adresáře (*CN=oddily,CN=konfigurace,DC=KorenovaDomenaStruktury*). Po vytvoření nových domén nebo oddílů adresáře aplikace se vytvoří rovněž objekt křížového odkazu v kontejneru Partitions. Pokud je hlavní operační server pro pojmenování domén nedostupný, nemůžete přidat ani odebrat objekty křížového odkazu.
- **Ověření instrukcí k přejmenování domény** – pokud používáte nástroj pro přejmenování domény Rendom.exe, pro přejmenování domény služby AD DS musí mít tento nástroj přístup k hlavnímu operačnímu serveru pro pojmenování domén. Po spuštění tohoto nástroje se do atributu *msDS-Update-Script* v objektu kontejneru Partitions (*CN=partitions,CN=configuration,DC=forestRootDomain)* v oddílu konfigurace adresáře zapíše skript zakódovaný v jazyce XML, který obsahuje instrukce

k přejmenování domény. Navíc nástroj Rendom.exe zapíše také nový název DNS všech přejmenovaných domén do atributu *msDS-DnsRootAlias* v objektu křížové vazby (třída *crossRef*) odpovídající dané doméně. Oba tyto objekty jsou uloženy v kontejneru Partitions a tento kontejner může být aktualizován pouze na řadiči domény, který plní roli hlavního operačního serveru pro pojmenování domén v příslušné doménové struktuře.

Hlavní server RID

Hlavní server RID je doménovou rolí hlavního operačního serveru. Používá se ke správě fondu RID, který vytváří nové objekty zabezpečení v doméně, jako jsou například uživatelé, skupiny a počítače. Pro každý objekt zabezpečení je vydán jedinečný identifikátor zabezpečení (SID), který zahrnuje identifikátor domény, který je stejný pro všechny identifikátory SID v dané doméně, a relativní identifikátor (RID), který je jedinečný pro každý objekt zabezpečení. Jelikož objekty zabezpečení lze vytvářet pouze na řadiči domény s kopií adresáře, do níž lze zapisovat, hlavní server RID zajišťuje to, aby dva řadiče domény nevydaly stejný identifikátor RID. Hlavní server RID vydá blok identifikátorů RID, zvaný *fond RID*, pro každý řadič domény v dané doméně. Pokud začne dostupných identifikátorů RID ve fondu RID na libovolném řadiči domény ubývat (jejich počet je menší než přibližně 100), hlavní server RID vydá požadavek na další blok identifikátorů RID. Jakmile je mu vyhověno, hlavní server RID vydá řadiči domény fond dalších přibližně 500 identifikátorů RID.

Pokud je hlavní server RID po určitou dobu nedostupný, proces vytváření nových účtů na konkrétních řadičích domény může být narušen. Mechanismus žádosti o nový blok identifikátorů RID je navržen tak, aby k takové situaci nedošlo, neboť požadavek je vydán před vyčerpáním všech dostupných identifikátorů RID ve fondu RID. Ovšem pokud je hlavní server RID v režimu offline a žádající řadič domény vyčerpá zbývající identifikátory RID, vytvoření účtu bude neúspěšné. Abyste znovu umožnili vytváření účtů, buď se musí řadič domény spravující roli hlavního serveru RID vrátit zpět do režimu online, nebo musí být role přenesena na jiný řadič domény v dané doméně.

Emulátor primárního řadiče domény

Role emulátor primárního řadiče domény (PDC) funguje jako primární řadič domény pro systémy starší než systém Windows 2000. Členské servery a klientské počítače se systémem Windows NT musí být schopny komunikovat s primárním řadičem domény, aby zpracovaly změny hesel. Kromě poskytnutí služeb pro starší klienty hraje primární řadič domény také důležitou roli při replikaci hesel.

Poznámka: Ve službě Active Directory systémů Windows 2000 a Windows 2003 je jednou z důležitých rolí emulace primárního řadiče domény to, aby sloužil jako primární řadič domény pro záložní řadiče domény nižší úrovně (se systémy Microsoft Windows NT verze 4 nebo 3.51). Jelikož systém Windows Server 2008 nepodporuje koexistenci s řadiči domény se systémy staršími než Windows 2000, tato funkce už nadále není důležitá.

I když v doméně neexistují žádné členské servery nebo klientské počítače se systémem Windows NT, role emulátoru primárního řadiče domény spočívá v údržbě aktualizací

hesel. Všechny změny hesel provedené na jiných řadičích domény v dané doméně jsou odeslány emulátoru primárního řadiče domény pomocí urgentní replikace.

Pokud ověření uživatele na řadiči domény jiném než na emulátoru primárního řadiče domény selže, ověření se znovu zkusí provést na emulátoru primárního řadiče domény. Pokud emulátor primárního řadiče domény akceptuje poslední změnu hesla daného účtu, ověření bude úspěšné. Pokud se uživatel úspěšně ověří na řadiči domény, kde předchozí pokus selhal, řadič domény uvědomí emulátor primárního řadiče domény o úspěšném ověření. Tím vynuluje čítač pro uzamčení účtu na emulátoru primárního řadiče domény pro případ, že se jiný klient pokusí ověřit stejný účet pomocí jiného řadiče domény. Emulátor primárního řadiče domény plní následují funkce:

- Slouží jako kořenový časový server pro danou doménu.
- Slouží jako původce zásad skupiny. Všechny změny objektů GPO jsou nejprve provedeny na emulátoru primárního řadiče domény a poté jsou replikovány na zbývající řadiče domény.
- Slouží jako původce změn hesel a uzamčení účtů, zajišťující konzistenci v doméně.

Hlavní server infrastruktury

Hlavní server infrastruktury je zodpovědný za aktualizaci odkazů typu skupina-uživatel mezi doménami. Tato role hlavního serveru infrastruktury zajišťuje, aby se provedené změny názvů objektů (změny atributu běžného názvu, *cn*) promítly v informacích o členství ve skupině pro skupiny umístěné v jiné doméně. Hlavní server infrastruktury udržuje aktuální seznam těchto odkazů a poté tyto informace replikuje na všechny ostatní řadiče domény v dané doméně. Pokud je hlavní server infrastruktury nedostupný, odkazy typu skupina-uživatel mezi doménami nebudou aktuální.

Přenos rolí hlavních operačních serverů

Role hlavních operačních serverů můžete přesouvat mezi řadiči domény buď kvůli lepší optimalizaci výkonu řadiče domény, nebo abyste nahradili řadič domény v případě, že vlastník role bude nedostupný. Tento proces bude záviset na přenášené roli. Tabulka 17.2 vypisuje nástroje použité k přenosu pěti rolí hlavního operačního serveru.

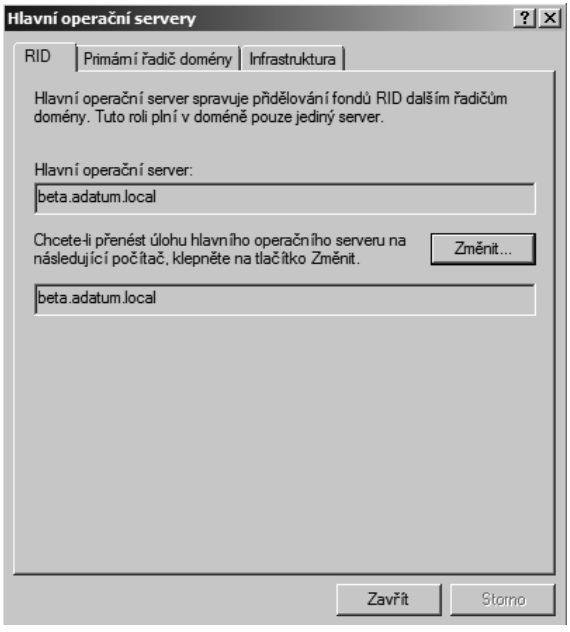
Tabulka 17.2: Nástroje pro správu rolí hlavního operačního severu

Role hlavního operačního serveru	Nástroj pro správu
Hlavní server schémat	Schéma služby Active Directory (Active Directory Schema)
Hlavní operační server pro pojmenování domén	Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains And Trusts)
Hlavní server RID, emulátor primárního řadiče domény a hlavní server infrastruktury	Uživatelé a počítače služby Active Directory (Active Directory Users And Computers)

Chcete-li přenést roli emulátoru primárního řadiče domény, postupujte podle následujících kroků:

1. Spusťte nástroj Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) ze složky Nástroje pro správu (Administrative Tools).

2. Klepněte pravým tlačítkem myši na uzlu domény a v místní nabídce zvolte příkaz Změnit řadič domény (Change Domain Controller).
3. Vyberte řadič domény, kterému chcete přiřadit roli emulátoru primárního řadiče domény. Klepněte na tlačítko OK.
4. Klepněte pravým tlačítkem myši na uzlu domény a v místní nabídce zvolte příkaz Hlavní operační servery (Operations Masters). Klepněte na kartu Primární řadič domény (PDC), abyste viděli server, který je aktuálně vybrán (řadič, který se stane emulátorem primárního řadiče domény), a řadič, který je aktuálním hlavním operačním serverem. (Viz obrázek 17.13.)



Obrázek 17.13: Změna hlavního operačního serveru role emulátoru primárního řadiče domény

5. Klepněte na tlačítko a poté klepněte na tlačítko OK.

Pro přenos role hlavního operačního serveru musí existovat připojení k aktuálnímu i zamýšlenému vlastníkovi role řadičů domény. V případě selhání serveru nemusí být vlastník aktuální role schopen dokončit přenos role. V takovém případě může danou roli převzít jiný řadič domény. Převzetí rolí hlavního operačního serveru není upřednostňovanou možností a mělo by být provedeno pouze v případě absolutní nevyhnutelnosti. Roli hlavního operačního serveru byste měli převzít, pouze pokud je jasné, že řadič domény, který je hostitelem této role, nebude delší dobu dostupný.

Poznámka: Role hlavního operačního serveru můžete přesunout na jiný řadič domény v dané doméně. Jedinou výjimkou při umístění hlavního operačního serveru je, že roli hlavního serveru infrastruktury byste neměli instalovat na řadič domény, který je rovněž serverem globálního katalogu, jestliže doménová struktura obsahuje více domén, ledaže by

každý řadič domény v dané doméně byl rovněž serverem globálního katalogu. Ve výchozím nastavení je první řadič domény v doménové struktuře rovněž serverem globálního katalogu a obsahuje roli hlavního serveru infrastruktury. Pokud v doméně nainstalujete druhý řadič domény a tento řadič domény není serverem globálního katalogu, Průvodce instalací služby Active Directory (Active Directory Domain Services Installation Wizard) vás během instalace služby AD DS vyzve k přesunutí hlavního serveru infrastruktury na nový řadič domény.

Převzetí rolí hlavního operačního serveru

V některých případech se můžete rozhodnout, že nové vytvoření řadiče domény, který selhal, by trvalo déle než doba, po kterou by mohla vaše síť fungovat bez hlavního operačního severu. Nebo byste se mohli rozhodnout, že vůbec nechcete obnovit řadič domény, ale raději byste vytvořili nový řadič domény a přenesli roli hlavního operačního severu na tento nový řadič domény. Přenos role hlavního operačního severu je snadný, pokud jsou oba řadiče domény v režimu online, protože řadiče domény mohou zaručit dokončení replikace před přenesením role. Ovšem pokud hlavní operační server selhal a vy potřebujete přesunout roli na jiný řadič domény, budete muset roli převzít.

Chcete-li převzetí role hlavního operačního serveru pomocí nástroje Ntdsutil, postupujte podle následujících kroků:

1. Otevřete příkazový řádek.
2. Na příkazovém řádku zadejte příkaz ntdsutil a stiskněte klávesu Enter.
3. Na příkazovém řádku Ntdsutil zadejte příkaz roles a stiskněte klávesu Enter.
4. Na příkazovém řádku Fsmo Maintenance zadejte příkaz connections a stiskněte klávesu Enter.
5. Na příkazovém řádku Server Connections zadejte příkaz connect to server NazevServeru, kde NazevServeru je názvem serveru, na který chcete umístit roli hlavního operačního serveru, a stiskněte klávesu Enter.
6. Na příkazovém řádku Server Connection zadejte příkaz quit a stiskněte klávesu Enter.
7. Na příkazovém řádku Fsmo Maintenance zadejte příkaz seize role, kde role je role hlavního operačního serveru, který chcete převzít, a stiskněte klávesu Enter. Platnými hodnotami parametru role jsou hodnoty schema master, domain naming master, infrastructure master, RID master a PDC.
8. Potvrďte upozornění. Server se nejprve pokusí provést běžný přenos zadané role hlavního operačního serveru. Pokud dojde k selhání kvůli nemožnosti kontaktování řadiče domény, role bude převzata.
9. Pomocí příkazu quit ukončete nástroj Ntdsutil.

Poznámka: K převzetí rolí emulátor primárního řadiče domény a hlavní server infrastruktury můžete rovněž použít nástroj Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).

Důležité: Před převzetím hlavního názvového serveru domény musíte řadič, který vlastní roli hlavního názvového serveru domény, zcela odpojit od sítě. Převzetí role hlavního názvového serveru domény je radikálním krokem, a neměli byste jej proto provádět, dokud nebude původní hlavní názvový server domény trvale mimo provoz. Před uvedením původního hlavního názvového serveru domény zpět do režimu online musíte nejprve znovu naformátovat spouštěcí disk a přeinstalovat systém Windows Server 2008.

Audit služby AD DS

Ve většině organizací nabízí služba AD DS centrální ověřování a službu ověřování adresáře. Většina síťových aplikací, pokud ne všechny, může záviset na tom, aby služba AD DS povolila uživatelům přístup nebo zabránila neautorizovaným uživatelům v přístupu k dané aplikaci. To znamená, že všechny změny ve službě AD DS mohou mít dalekosáhlé důsledky pro vaši síť. Abyste měli jistotu, že tyto změny mohou provádět pouze oprávnění uživatelé, musíte nakonfigurovat všechny účty pro správu s minimálními oprávněními potřebnými k provedení požadovaných úloh. Druhou součástí pro správu změn služby AD DS je audit změn provedených na řadičích domény. Auditováním změn provedených na řadičích domény můžete zjistit, kdo je zodpovědný za změny adresáře a kdy byly tyto změny provedeny.

Konfigurace zásad auditu

Systém Windows Server 2008 zavádí některé důležité změny v provádění auditu na řadičích domény. V systémech Windows 2000 Server a Windows Server 2003 jste měli pouze jednu možnost zásady auditu: Auditovat přístup k adresářové službě (Audit directory service access), která určovala, zda byl audit událostí adresářové služby povolen, nebo zakázán. V systému Windows Server 2008 jsou tyto zásady rozděleny do čtyřech podkategorií:

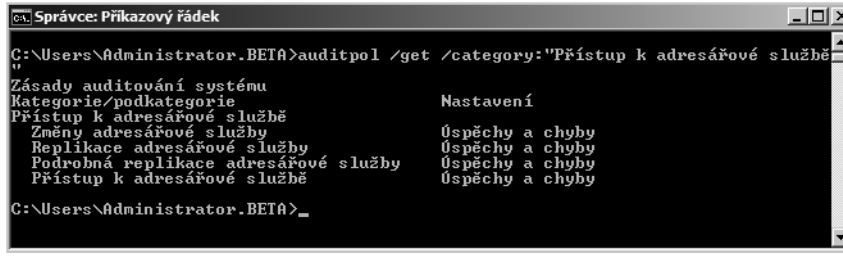
- Přístup k adresářové službě (Directory Service Access)
- Změny adresářové služby (Directory Service Changes)
- Replikace adresářové služby (Directory Service Replication)
- Podrobná replikace adresářové služby (Detailed Directory Service Replication)

Tyto podkategorie nejsou viditelné prostřednictvím nástroje Editor správy zásad skupiny (Group Policy Management Editor). Pro zobrazení a konfiguraci těchto podkategorií použijte nástroj příkazového řádku Auditpol.exe. Pro zobrazení aktuálních nastavení auditování přístupu k adresářové službě zadejte příkaz **Auditpol /get /category:"Přístup k adresářové službě"**.

Obrázek 17.14 zobrazuje výstup tohoto příkazu s výchozími nastaveními.

Z hlediska auditu zabezpečení je nejdůležitější novou funkcí podkategorie Změny adresářové služby (Directory Service Changes). Tato nová podkategorie přidává následující funkce:

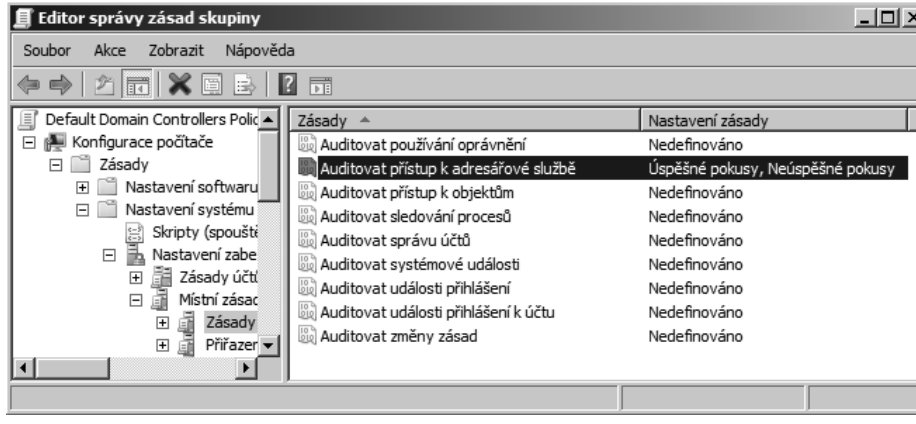
- Pokud změníte atribut v určitém objektu, služba AD DS zaznamená do protokolu předchozí a aktuální hodnoty atributu. Pokud má atribut více než jednu hodnotu, do protokolu se zaznamenají pouze hodnoty, které se následkem modifikace změnily.



Obrázek 17.14: Zobrazení zásad auditu adresářové služby

- Pokud vytvoříte nový objekt, hodnoty atributů, které jsou v době vytváření obsazeny, se zaznamenají do protokolu. Pokud uživatel přidá atributy během jejich vytváření, hodnoty těchto nových atributů se zaznamenají do protokolu. Ve většině případů služba AD DS přiřadí atributům výchozí hodnoty (například *samAccountName*). Hodnoty těchto systémových atributů se do protokolu nezaznamenávají.
- Pokud dojde k přesunutí objektu, předchozí a nové umístění (rozlišující název) se zaznamená do protokolu u přesunů v rámci domény. Pokud dojde k přesunutí objektu do jiné domény, na řadiči domény v cílové doméně se vygeneruje událost vytvoření.
- Pokud dojde k obnovení odstraněného objektu, umístění, do nějž je tento objekt přesunut, se zaznamená do protokolu. Navíc pokud uživatel přidá, změní nebo odstraní atributy při provádění operace obnovení odstraněného objektu, hodnoty těchto atributů se zaznamenají do protokolu.

Ve výchozím nastavení není kategorie auditu přístupu Auditovat přístup k adresářové službě (Audit directory service access) povolena v organizační jednotce Default Domain Controllers, ovšem podkategorie Přístup k adresářové službě (Directory Service Access) povolena je. Tyto zásady auditu se zaznamenají do protokolu při přístupu správce k objektům ve službě AD DS, avšak změny v těchto objektech se do protokolu nezaznamenávají. Chcete-li povolit audit kategorie Změny adresářové služby (Directory Services Changes), můžete zvolit možnost povolení zásady Auditovat přístup k adresářové službě (Audit directory service access) v zásadách auditu objektu Default Domain Controllers Policy. Pokud tuto možnost povolíte, dojde rovněž k povolení všech podkategorií. (Viz obrázek 17.15.)



Obrázek 17.15: Konfigurace auditu adresářové služby

Chcete-li povolit pouze podkategorii Změny adresářové služby (Directory Service Changes), musíte použít nástroj příkazového řádku Auditpol.exe a spustit následující příkaz:

```
auditpol /set /subcategory:"Změny adresářové služby" /success:enable
```

Systém Windows Server 2008 představuje podkategorie také v jiných kategoriích auditu. Tyto kategorie, podkategorie a výchozí nastavení specifických nastavení auditu služby AD DS jsou uvedeny v tabulce 17.3. K zobrazení těchto nastavení auditu použijte příkaz **Auditpol /get /category:***.

Tabulka 17.3: Konfigurace nastavení zásad auditu řadiče domény

Kategorie	Podkategorie	Výchozí nastavení
Auditovat události přihlášení (Audit logon events)	Přihlášení (Logon)	Úspěšné pokusy a Neúspěšné pokusy
Auditovat události přihlášení (Audit logon events)	Odhlášení (Logoff)	Úspěšné pokusy
	Uzamčení účtu (Account Lockout)	Úspěšné pokusy
Auditovat události přihlášení (Audit logon events)	Hlavní režim protokolu IPsec (IPsec Main Mode), Rozšířený režim protokolu IPsec (IPsec Extended Mode), Rychlý režim protokolu IPsec (IPsec Quick Mode)	Bez auditování
Auditovat události přihlášení (Audit logon events)	Zvláštní přihlášení (Special Logon)	Úspěšné pokusy
Auditovat události přihlášení (Audit logon events)	Jiní události přihlášení nebo odhlášení (Other Logon/Logoff events)	Bez auditování
Auditovat události přihlášení (Audit logon events)	Server NPS (Network Policy Server)	Úspěšné pokusy a Neúspěšné pokusy
Změna zásad auditu (Audit policy change)	Změna zásad auditu (Audit Policy Change)	Úspěšné pokusy
Změna zásad auditu (Audit policy change)	Změna zásad ověřování (Authentication Policy Change)	Úspěšné pokusy
Změna zásad auditu (Audit policy change)	Změna zásad autorizace (Authorization Policy Change), Změna zásad úrovně pravidla MPSSVC (MPSSVC Rule-Level Policy Change), Změna zásad architektury Filtering Platform (Filtering Platform Policy Change), Jiné události změny zásad (Other Policy Change Events)	Bez auditování
Auditovat správu účtů (Audit account management)	Správa uživatelských účtů (User Account Management)	Úspěšné pokusy
Auditovat správu účtů (Audit account management)	Správa účtů počítače (Computer Account Management)	Úspěšné pokusy
Auditovat správu účtů (Audit account management)	Správa skupiny zabezpečení (Security Group Management)	Úspěšné pokusy
Auditovat správu účtů (Audit account management)	Správa distribučních skupin (Distribution Group Management), Správa skupin aplikací (Application Group Management), Jiné události správy účtů (Other Account Management Events)	Bez auditování

Kategorie	Podkategorie	Výchozí nastavení
Auditovat přihlášení k účtu (Audit account logon events)	Operace lístku služby Kerberos (Kerberos Service Ticket Operations)	Úspěšné pokusy
Auditovat přihlášení k účtu (Audit account logon events)	Jiné události přihlášení k účtu (Other Account Logon Events)	Bez auditování
Auditovat přihlášení k účtu (Audit account logon events)	Ověřovací služba Kerberos (Kerberos Authentication Service)	Úspěšné pokusy
Auditovat přihlášení k účtu (Audit account logon events)	Ověření pověření (Credential Validation)	Úspěšné pokusy

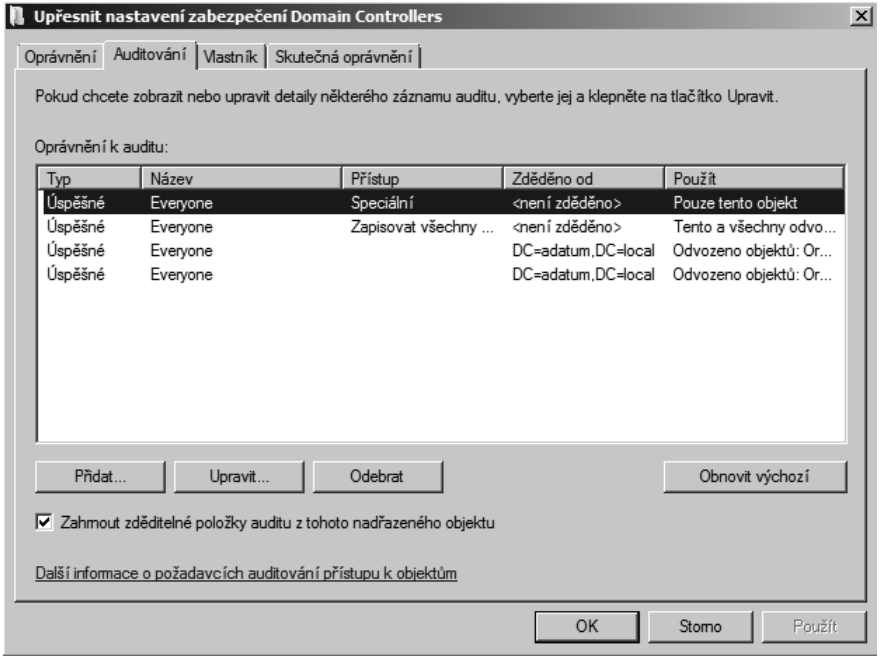
Ve většině případů platí, že pokud je cílem vašich zásad auditu auditovat aktivitu správce ve službě AD DS, měli byste přijmout výchozí nastavení auditu řadič domény. Pokud používáte zásady auditu z jiných důvodů, například jako detekci vniknutí, možná chcete auditovat také selhání událostí, jako jsou události přihlášení nebo události správy účtů. Ve výchozím nastavení platí, že pokud povolíte audit jakékoliv kategorie, povolíte tím také audit ve všech jejích podkategoriích.

Povolení auditu změn služby AD DS

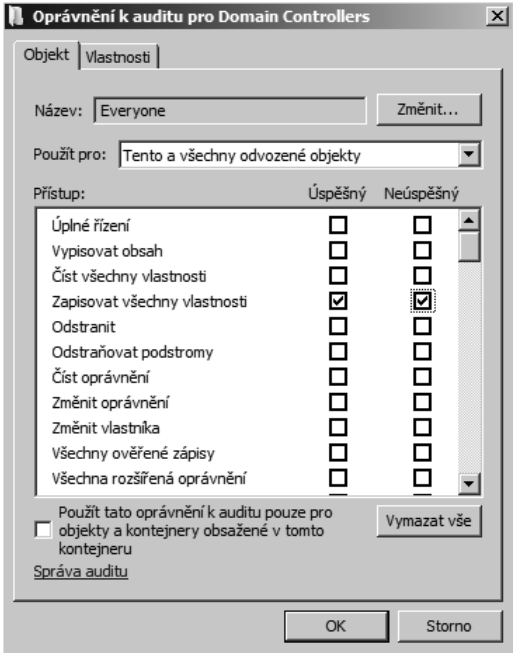
Konfigurace zásad auditu je pouze prvním krokem při povolení auditu služby AD DS. Po konfiguraci zásad auditu musíte nakonfigurovat seznam řízení auditování přístupu (SACL) pro každý objekt, abyste povolili auditování. Chcete-li auditovat změny v objektech ve službě AD DS, povolte audit organizační jednotky Domain Controllers v nástroji Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).

Chcete-li povolit audit organizační jednotky Domain Controllers, postupujte podle následujících kroků:

1. Otevřete nástroj Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).
2. Klepněte v nabídce na příkaz Zobrazit (View) a poté klepněte na příkaz Upřesňující funkce (Advanced Features).
3. Klepněte pravým tlačítkem myši na organizační jednotce Domain Controllers a poté klepněte na příkaz Vlastnosti (Properties).
4. V dialogu Vlastnosti (Properties) klepněte na kartu Zabezpečení (Security), klepněte na tlačítko Upřesnit (Advanced) a poté klepněte na kartu Auditování (Auditing), znázorněnou na obrázku 17.16.
5. Klepněte na tlačítko Přidat (Add) a v dialogu Vybrat objekt typu: uživatel, počítač nebo skupinu (Select User, Computer, Or Group) zadejte Everyone a poté klepněte na tlačítko OK. Volbou skupiny Everyone můžete auditovat všechny změny provedené ve službě AD DS kterýmkoliv uživatelem.
6. V dialogu Oprávnění k auditu pro Domain Controllers (Auditing Entry for Domain Controllers) (viz obrázek 17.17) zaškrtněte políčka Úspěšný (Successful) i Neúspěšný (Failed) u položky Zapisovat všechny vlastnosti (Write All Properties) a poté dvakrát klepněte na tlačítko OK.

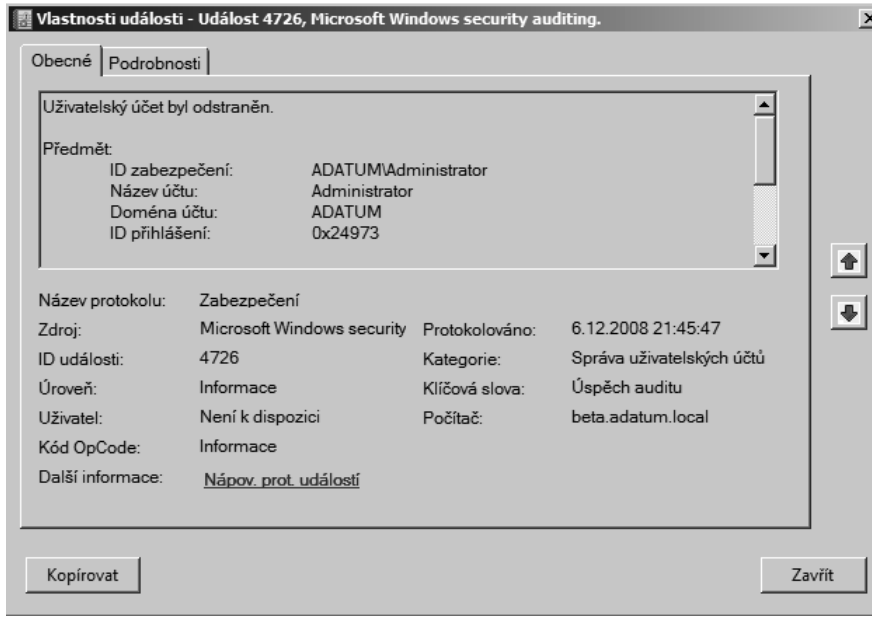


Obrázek 17.16: Konfigurace auditu organizační jednotky Domain Controllers



Obrázek 17.17: Auditování všech změn provedených ve službě AD DS

Když povolíte audit kategorie Změny adresářové služby (Directory Service Changes), všechny změny provedené ve službě AD DS se zobrazí v protokolu Zabezpečení (Security), viz obrázek 17.18.



Obrázek 17.18: Změny služby AD DS jsou znázorněny v protokolu Zabezpečení (Security)

Shrnutí

Služba AD DS je neodmyslitelnou součástí síťové infrastruktury podniku se systémem Windows Server 2008 a její údržba je důležitou součástí práce správce sítě. Ačkoliv služba AD DS nevyžaduje po své instalaci velký objem údržby, je třeba strávit určitý čas vytvářením plánu zálohování a obnovení a pochopit procedury provádění úloh, jako je správa rolí hlavních operačních serverů a konfigurace auditu.

V další kapitole se zaměříme na základní nastavení a správu infrastruktury TCP/IP.