Údržba Active Directory

[Povinné]

Ani sebelepší konfigurace **Active Directory** nemění nic na faktu, že je potřeba pravidelně provádět její údržbu. Také je důležité si uvědomit, že údržba se netýká jen databáze **Active Directory**, ale obecně všeho co s ní souvisí. Nejde tedy jen o údržbu identit **Active Directory**, jako jsou účty uživatelů a počítačů, nutných pro autentizaci, **GPO** objektů, potřebných pro aplikaci zásad skupiny na tyto uživatele a počítače, nebo objektů míst, spojení a linek, jenž instruují **KCC** a **ISTG**, jak vytvářet replikační topologii. Je také nutné zajistit přístup ke zdrojům a službám. Počítače musí být schopny kontaktovat řadiče domény a jiné servery poskytující požadované služby (např. *file* a *web* servery), což vyžaduje správné nastavení systému **DNS** a objektů podsítí. Důležitá je také bezpečnost, jak z pohledu zabezpečení přístupu ke zdrojům, tak zabezpečení samotných řadičů domény[1]. Řadiče domény také musí být schopny rychle a spolehlivě obsluhovat požadavky klientů, měly by být tedy také pravidelně monitorovány. To je jen část úkolů, které lze zařadit do celkové údržby **Active Directory**.

Údržba databáze Active Directory

[Povinné]

Údržba databáze **Active Directory** byla v minulosti značně problematická. V předchozích verzích systému Windows Server byla totiž role řadiče domény monolitická. Jediná možnost jak zastavit službu **Active Directory** byla zastavit celý řadič domény. V praxi to znamenalo, že v případě údržby databáze **Active Directory** bylo potřeba vypnout řadič domény a nastartovat ho v režimu obnovení adresářových služeb (*Directory Services Repair Mode*), ve kterém nejsou spuštěny služby **Active Directory**. Díky tomu nebylo možné jakkoliv automatizovat údržbu databáze **Active Directory**. Windows Server 2008 přinesl v tomto ohledu zásadní změnu. Role řadiče domény je nyní již standardní (ovladatelná) služba, jenž může být kdykoliv zastavena, restartována nebo spuštěna.

Na rozdíl od standardních služeb je zde ovšem jedno omezení. Aby bylo možné zastavit službu **AD DS** (*Active Directory Domain Services*), je potřeba mít v síti přítomen další řadič domény. Každý řadič domény se před zastavením služby **AD DS** nejprve pokusí spojit s nějakým jiným řadičem domény a pouze pokud se mu to podaří, zastaví službu **AD DS**. Toto chování zajišťuje, že je v síti vždy přítomen alespoň jeden řadič domény.

Potřeba provádění údržby databáze **Active Directory** je následující. Při přidávání nových záznamů (objektů) do databáze dochází k alokaci místa pro jejich uložení. V případě mazání záznamů ale není toto alokované místo uvolněno. Pro jeho uvolnění musí být provedeno tzv. *zkompaktnění*[2](*compaction*) databáze. **Active Directory** sice provádí údržbu své databáze, ale pouze ve formě přesunu záznamů, aby byly lépe (rychleji) přístupné, neuvolňuje tedy žádné místo.

Ochrana Active Directory

[Povinné]

Ochrana **Active Directory** se samozřejmě týká primárně ochrany dat, tedy ochrany objektů uložených v databázi **Active Directory**. Asi nejvíce kritické jsou bezpečnostní objekty (*security principals*). Každý bezpečnostní objekt (účet uživatele či počítače, skupina apod.) obsahuje unikátní **SID** (*security identifier*) identifikátor. Tento identifikátor je generován náhodně pro každý vytvářený bezpečnostní objekt. Pokud je tedy nějaký bezpečnostní objekt smazán a poté vytvořen objekt nový, se stejnými hodnotami atributů, budou jejich **SID** identifikátory odlišné a pro **Active Directory** to

[1] Nejde jen o zabezpečení systému, který běží na řadiči domény, či uživatelských účtů, které se mohou k tomuto řadiči přihlásit, ale i o fyzické zabezpečení. Obecně se doporučuje, aby se řadiče domény spravovaly jen vzdáleně a byly uloženy na bezpečném místě, kde má přístup jen několik pověřených osob

[2] *Zkompaktnění* databáze je proces, při kterém se nejprve provede *defragmentace* databáze, následovaná její minimalizací. V případě **Active Directory** databáze, souboru **Ntds.dit**, je výsledkem *defragmentace* přesun veškerých dat na začátek tohoto souboru následovaný minimalizací tohoto souboru (ořezání konce souboru, kde je nyní situováno všechno, dříve alokované, neuvolněné místo)

budou dva zcela odlišné objekty. Jednou smazaný bezpečnostní objekt není tedy možné již znova vytvořit, tak aby měl zachovány informace o příslušnosti do skupin, o přístupu ke zdrojům, o uložených heslech a certifikátech a o řadě dalších věcí. Všechny tyto informace jsou ztraceny smazáním bezpečnostního objektu a proto je důležité účty a podobné objekty raději zakazovat než mazat. Takto nehrozí nebezpečí jejich zneužití a mohou být v případě potřeby opět použity (např. když by se uživatel vrátil, nebo jiný uživatel nastoupil na jeho místo).

Díky replikaci poskytuje **Active Directory** dobrou ochranu proti nečekané ztrátě dat[3], veškerá data jsou vlastně zálohována na každém z řadičů domény. Replikace ale může způsobit také problémy. Pokud je nějaký objekt vymazán z **Active Directory**, dojde k jeho vymazání i na všech ostatních řadičích domény. Pak je jedinou možností obnova **Active Directory** databáze. **Active Directory** ovšem nabízí i jiné možnosti ochrany nebo následné obnovy dat:

- **Ochrana objektů před smazáním**. Každý vytvořený objekt **Active Directory** může být chráněn proti smazání. Tato ochrana se zapíná na záložce Object[4] zaškrtnutím možnosti Protect object from accidental deletion. Většina vytvářených objektů má tuto možnost po vytvoření zakázanou, jen kontejnery jako organizační jednotky ji mají povolenou pro větší ochranu struktury **Active Directory**. Objekt chráněný před smazáním nemůže být smazán ani přesunut, nejdříve musí být vždy zrušena jeho ochrana. Prakticky tato ochrana nedělá nic jiného, než že nastaví dvě Deny oprávnění (Deny Delete a Deny Delete subtree) pro skupinu Everyone.
- **Auditovaní změn**. Systémy Windows Server 2008 a novější protokolují celkem čtyři kategorie přístupu k adresářovým službám. Z hlediska ochrany objektů je asi nejdůležitější auditovaní změn v **Active Directory** (*Directory Service Changes*), jenž protokoluje staré a nové hodnoty atributů objektů, které byly vytvořeny, změněny, přesunuty či obnoveny. Tyto hodnoty jsou zaznamenávány do protokolu událostí adresářových služeb (*Directory Services Event Log*). Pro každou změnu jsou zaprotokolovány alespoň dvě události, kdy první obsahuje starou hodnotu a druhá novou hodnotu nějakého atributu. Tyto informace mohou být použity pro opravu nesprávně změněných hodnot atributů objektů.
- **Obnova objektů**. Pokud je nějaký objekt **Active Directory** smazán, není ihned fyzicky odstraněn z databáze **Active Directory**, ale je přesunut, na určitou dobu, do speciálního kontejneru Deleted Objects. Objekty obsažené v tomto kontejneru je možné kdykoliv obnovit a označují se jako tzv. *tombstoned* objekty (smazané, ale ne odstraněné objekty, které se od původních objektů liší nastaveným atributem **isDeleted**). Jelikož je kontejner Deleted Objects skrytý, je pro obnovu potřeba používat nástroje, které vidí i skryté kontejnery jako např. **Ldp.exe** nebo jiné speciální nástroje. Ve výchozím nastavení jsou *tombstoned* objekty uchovávány 180 dní, pokud není tato doba změněna nebo nejsou provedeny některé operace pročišťující databázi **Active Directory**. I přesto, že obnovené objekty mají zachovány hodnoty většiny svých atributů, včetně **SID** identifikátorů, některé informace, jako např. členství ve skupinách, nemusí být již přítomny.
- **Záloha a obnova databáze**. Systém Windows Server od verze 2008 obsahuje **Windows Server Backup**, jenž lze použít k zálohování nebo obnovení databáze **Active Directory**.

Záloha a obnova databáze Active Directory [Povinné]

Obnova objektů nemusí být často ideální metodou pro obnovu dat. Obnovené objekty obecně neobsahují veškeré informace a hodnoty atributů, jenž měly před svým smazáním. Je potřeba je znova doplnit, aby se objekt dostal do stejného stavu, v jakém byl před svým smazáním. Tyto informace a hodnoty již ale nemusí být známy. Kromě toho, v případě velkého množství objektů, ani nemusí být možné je všechny obnovit. Obnovením zálohy databáze **Active Directory** se obnoví

[3] Nečekanou ztrátou dat je myšleno např. selhání HDD, tedy ztráta způsobena mimo systém **Active Directory**
[4] Tato záložka je viditelná pouze, pokud jsou povolené pokročilé možnosti zobrazení (Advanced Features)

veškeré objekty spolu se všemi jejich atributy a také i všechny ostatní informace jako např. členství ve skupinách. Pro zálohování a obnovení databáze **Active Directory** lze použít **Windows Server Backup**.

Velkým problémem v předchozích verzích systému Windows Server byla nemožnost zobrazení obsahu jednotlivých záloh databáze **Active Directory**. Nešlo tedy nijak určit, zda jsou objekty, které jsou potřeba obnovit, opravdu přítomny v dané záloze. Windows Server od verze 2008 obsahuje nástroj **AD DS Database mounting tool**, jenž umožňuje zobrazit a procházet obsah záloh databáze **Active Directory**.

Z hlediska zálohování nemusí být zálohována jen samostatná databáze **Active Directory**. **Window Server Backup** umožňuje zálohovat celý server (včetně operačního systému) nebo jen jeho specifické části jako např. data stavu systému (*System State Data*). Z hlediska obnovy databáze **Active Directory** je potřeba rozlišovat dva typy obnovy:

- **Autoritativní obnova**. Při autoritativní obnově budou data obnovena na daný řadič domény a tento řadič domény aktualizuje pomocí replikace data na všech ostatních řadičích domény.
- **Neautoritativní obnova**. Při neautoritativní obnově budou opět data obnovena na daný řadič domény, ale tato data budou aktualizována replikací z ostatních řadičů domény, jakmile bude daný řadič domény zpět k dispozici (*online*).

Kromě zálohy a obnovy databáze **Active Directory** nabízí Windows Server ještě možnost tzv. instalace z média (**IFM**, *Install From Media*). **IFM** umožňuje vytvořit speciální kopii databáze **Active Directory** (souboru **Ntds.dit**), jenž může být použita při instalaci nového řadiče domény jako alternativní zdroj dat namísto replikace. Tímto se může výrazně snížit množství replikovaných dat při instalaci daného řadiče domény.

Záloha databáze Active Directory [Povinné]

Oproti předchozím verzím systému Windows Server došlo u Windows Server 2008 k několika dosti podstatným změnám ohledně zálohování. Navíc také Windows Server 2008 R2 přinesl další úpravy a novinky v této oblasti. Pro maximálně efektivní vytváření záloh je vhodné dobré znát veškerá omezení a možnosti zálohování.

Zálohy mohou být vytvářeny dvěma způsoby. Buď pomocí **Windows Server Backup** nebo pomocí nástroje **Wbadmin.exe** (*Windows Backup Administration*). Oba tyto nástroje jsou součásti (*features*) systému Windows Server 2008 (a novějších) a musí být před prvním použitím nejprve nainstalovány. Zálohy mohou být vytvářeny automaticky (v pravidelných intervalech) i manuálně. Automatické zálohy ale nemohou být prováděny členy skupiny Backup Operators, ti mohou provádět jen manuální zálohování. Jen členové skupiny Administrator na daném počítači mohou nastavit automatické zálohování, což v případě normálních řadičů domény jsou ale všichni členové skupiny Domain Admins, tedy správci domény.

Ve Windows Server lze provádět celkem dva typy záloh:

- **Záloha celého serveru** (*Full Server Backup*). Tato záloha zahrnuje veškerá data všech oddílů pevných disků daného serveru. Není možné zálohovat jednotlivé soubory ani adresáře, což se brzy ukázalo jako velice omezující a vedlo k zbytečně velkým zálohám. Od Windows Server 2008 R2 již umožňuje vybírat i jednotlivé soubory a adresáře. Navíc lze specifikovat soubory, které nebudou zahrnuty do zálohy na základě jejich typu (přípony) nebo cesty.
- **Záloha kritických oddílů** (*Critical Volume Backup*). Tato záloha obsahuje veškerá data potřebná pro obnovu doménových služeb **Active Directory** (**AD DS**). Přesněji tento typ zálohy zahrnuje data následujících oddílů:
  - **Systémového oddílu**. Oddíl obsahující kořenový adresář systému Windows.
  - **Bootovacího oddílu**. Oddíl obsahující soubory nutné pro start systému Windows. Ve většině případů je tento oddíl totožný s oddílem systémovým.
  - **Oddílu, jenž obsahuje databázi Active Directory**. Ve výchozím nastavení to je systémový oddíl.

- **Oddílu zahrnujícího protokoly Active Directory**. Ve výchozím nastavení opět systémový oddíl.
- **Oddílu hostujícího adresář SYSVOL**. Ve výchozím nastavení zase systémový oddíl.

Zálohy nemohou být uloženy na páskové jednotky ani na USB Flash disky, pouze na síťové a odnímatelné (externí) disky nebo na média CD a DVD. Od Windows Server 2008 R2 je možné provést zálohu také na oddíly interních disků, do sdíleného adresáře a také na virtuální a dynamické disky. Při uložení zálohy do sdíleného adresáře bude ovšem vždy udržována pouze jediná verze zálohy.

Windows Server 2008 R2 navíc zjednodušil správu a práci s úplnými a inkrementálními zálohami. **Windows Server Backup** nyní vytváří ve výchozím nastavení inkrementální zálohy, které se chovají jako úplné zálohy. Veškerá data lze tedy obnovit z jediné zálohy, i když je tato záloha jen inkrementální. Dále také dochází k automatickému mazání starých záloh, bez potřeby manuálního zásahu uživatele. Kromě toho také obsahuje sadu nástrojů (*cmdletů*) pro **PowerShell**, které umožňují automatizovat zálohování pomocí skriptů. Případně lze také využít nástroj **Wbadmin.exe**, jenž poskytuje nyní stejné možnosti jako **Windows Server Backup**.

Záloha stavu systému

[Povinné]

Stav systému (*System State*) je sada dat potřebná pro chod systému Windows a pro plnění některých rolí. V případě řadiče domény zahrnuje stav systému:

- **Registr**.
- **Databázi registrovaných COM+ tříd** (*COM+ Class Registration database*).
- **Bootovací soubory**.
- **Systémové soubory, které jsou pod ochranou zdrojů systému Windows** (**WRP**, *Windows Resource Protection*). Zde standardně patří většina systémových souborů systému Windows.
- **Databázi Active Directory**. Tedy soubor **Ntds.dit**.
- **Adresář SYSVOL**.

Pokud jsou na serveru nainstalovány i jiné role, stav systému bude vždy obsahovat první čtyři výše zmíněné části a dále:

- **Databázi certifikačních služeb Active Directory** (**AD CS**). Pokud server plní roli **AD CS** (*Active Directory Certification Services*).
- **Informace o výpočetním klusteru**. Pokud je nainstalována služba Microsoft Failover Cluster.
- **Konfigurační soubory IIS**. Pokud server plní roli webového serveru (*Web Server*).

Ve Windows Server 2008 bylo možné zálohovat stav systému pouze pomocí nástroje **Wbadmin.exe**, nešlo tedy pro zálohování použít **Windows Server Backup**. Ten sice umožňoval zálohovat stav systému, ale pouze v rámci zálohování celých oddílů disků. **Windows Server Backup** bylo ale možné využít pro obnovu pouze stavu systému (bez ostatních dat ze zálohovaných oddílů).

Windows Server 2008 R2 přinesl v tomto ohledu podstatná zlepšení. **Windows Server Backup** tak nyní umožňuje zálohovat stav systému samostatně. Navíc lze se stavem systému uložit i další data. Dále je také možné vytvářet inkrementální zálohy stavu systému. Tyto zálohy jsou rychlejší a vyžadují méně místa. Inkrementální zálohy využívají stínové kopie (*shadow copies*) pro verzování různých verzí souborů namísto jednotlivých adresářů pro každou verzi souboru.

Obnova databáze Active Directory

[Povinné]

I přesto, že od Windows Server 2008 lze roli řadiče domény (**AD DS** službu) ovládat jako standardní službu, nelze tuto službu jednoduše zastavit a provést obnovu databáze **Active Directory**. Obnovu je možné provést pouze v prostředí **WinRE** (*Windows Recovery Environment*) nebo v **DSRM** (*Directory Services Restore Mode*) režimu.

V **DSRM** režimu lze provádět jen autoritativní a neautoritativní obnovy databáze **Active Directory**. Tento režim je přístupný v pokročilých možnostech bootování (*Advanced Boot Options*) na všech řadičích domény a k nastartování řadiče domény v tomto režimu je potřebné heslo pro **DSRM** režim. Toto heslo se nastavuje při povyšování serveru do role řadiče domény a změnit lze pouze po nastartování řadiče domény v **DSRM** režimu.

WinRE prostředí umožňuje provádět obnovy celého systému (včetně databáze **Active Directory**, je-li přítomná). **WinRE** prostředí může být buď nainstalováno lokálně (stejně jako např. konzole pro obnovu) nebo spuštěno z instalačního média.

Před obnovou databáze **Active Directory** je vždy vhodné nejprve zjistit, zda daná záloha obsahuje potřebná data (objekty). K tomuto účelu lze nyní využít nástroj **AD DS Database mounting tool**. Tento nástroj pracuje se snímky (*snapshots*) databáze **Active Directory** a umožňuje zobrazit jejich obsah. Snímky jsou vytvářeny při každé záloze databáze **Active Directory** a jsou identifikovány pomocí **GUID**. Nástroj **AD DS Database mounting tool** je součástí nástroje **ntdsutil.exe**.

Samotnou obnovu databáze **Active Directory** lze pak provést neautoritativně nebo autoritativně. První typ obnovy slouží hlavně v případech externího poškození databáze (např. selháním disku), kdy nedošlo ke ztrátě dat **Active Directory** (data jsou pořád přítomná na ostatních řadičích domény), ale pouze k poškození dat u jednoho řadiče domény. Po obnovení těchto dat jsou tato data aktualizována z ostatních řadičů domény. Druhý typ slouží k obnovení ztracených dat **Active Directory**. Takových dat, která již nejsou přítomná na žádném řadiči domény. Od neautoritativní obnovy se liší pouze tím, že po obnově jsou data označena jako autoritativní. V praxi to znamená nastavení čísla **USN** (*Update Sequence Number*), jenž říká ostatním řadičům domény, že jsou tato data novější než stávající. Navíc u obou typů obnovy nemusí být obnovena celá databáze, je možné obnovit pouze její část.

Ochrana řadičů domény virtualizací [Volitelné]

Řadiče domény jsou ideální kandidáti pro virtualizaci pomocí **Hyper-V**, jelikož poskytují čistě síťové služby. Virtuální stroje je mnohem jednodušší ochraňovat, obnovovat a obecně s nimi jakkoliv manipulovat. Pokud selže virtuální stroj plnící roli řadiče domény, stačí se vrátit k jeho předchozí verzi, nastartovat ji a nechat replikaci provést aktualizaci **Active Directory**. Tento postup zajišťuje asi nejrychlejší a nejsnadnější obnovu **Active Directory**.

Ochrana disků virtuálních strojů, které jsou normálními soubory, může být navíc zajištěna pomocí **VSS** (*Volume Shadow Copy Service*). **VSS** umožňuje automaticky vytvářet snímky obsahu těchto disků v pravidelných intervalech. Pokud dojde k poškození dat na nějakém z těchto disků, lze se jednoduše vrátit k jeho dřívější verzi přes záložku Předchozí verze (*Previous Versions*) ve vlastnostech souboru, jenž reprezentuje daný disk virtuálního stroje.

Služba **VSS** by vždy měla běžet na serverech, na kterých běží virtuální stroje. **VSS** je systém, který umožňuje provádět zálohy oddílů, i když aplikace stále na tyto oddíly zapisují. Je implementován jako sada **COM** rozhraní a je k dispozici i u **Server Core** instalace.

Active Directory koš [Povinné]

Active Directory koš, představený ve Windows Server 2008 R2, značně rozšiřuje možnosti uchovávání a obnovy omylem smazaných objektů **Active Directory** bez nutnosti jejich obnovy ze záloh, restartování **AD DS** služeb nebo i celého řadiče domény. Pokud je **Active Directory** koš povolen, přímé (*non-link-valued*) i nepřímé (*link-valued*) atributy smazaných objektů **Active Directory** jsou zachovány a obnoveny do přesně stejného logického stavu, ve kterém byly v okamžiku těsně před svým smazáním. Tedy, na rozdíl od obnovy *tombstoned* objektů, jsou kromě hodnot atributů těchto objektů obnoveny také např. informace o členství ve skupinách a k nim vázané oprávnění pro přístup ke zdrojům. Jsou tedy obnoveny i informace, jenž nejsou přímo uloženy v rámci daných objektů, ale jsou s nimi nějak svázány.

Active Directory koš je možné použít jak pro doménové služby **Active Directory** (**AD DS**), tak i pro adresářové služby **Active Directory** (**AD LDS**) a ve výchozím nastavení je zakázán. Pro povolení **Active Directory** koše je potřeba mít funkční úroveň lesa Windows Server 2008 R2 nebo vyšší a aktualizované schéma **Active Directory**[5]. Potřebné aktualizace schématu se provádějí během přípravy lesa příkazem **adprep /forestprep**, během přípravy domény příkazem **adprep /domainprep /gpprep** a v případě existence **RODC** řadičů v doméně ještě vykonáním příkazu **adprep /rodcprep**. U **AD LDS** se místo schématu musí aktualizovat **AD LDS** konfigurace pomocí nástroje **Ldifde.exe**. Povolení **Active Directory** koše je nevratná operace, jakmile je tento koš jednou povolen, nelze ho již vypnout.

Pokud je **Active Directory** koš povolen, rozlišují se celkem čtyři typy objektů **Active Directory**:

- **Živý objekt** (*Live object*). Živé objekty jsou všechny nesmazané objekty v **Active Directory**.
- **Smazaný objekt** (*Deleted object*). Pokud je živý objekt smazán, stane se z něj smazaný objekt (stane se tzv. *logicky smazaným* objektem). Veškeré přímé a nepřímé atributy daného objektu jsou zachovány a je přesunut do kontejneru Deleted Objects. V tomto kontejneru zůstává po dobu životnosti smazaných objektů (ve výchozím nastavení 180 dnů). Během této doby lze objekt obnovit (*undelete*) nebo autoritativně obnovit (*restore*).
- **Recyklovaný objekt** (*Recycled object*). Pokud vyprší doba životnosti smazaného objektu, stane se recyklovaným objektem. Většina atributů tohoto objektu je odstraněna. Které atributy mají být ponechány, je možné specifikovat ve schématu **Active Directory**. Recyklovaný objekt je stále umístěn v kontejneru Deleted Objects, ale není viditelný, a zůstává v něm, dokud nevyprší jeho doba životnosti (ve výchozím nastavení 180 dnů).
- **Odstraněný objekt** (*Physically deleted object*). Pokud vyprší doba životnosti recyklovaného objektu, je tento objekt fyzicky smazán z databáze **Active Directory**. O odstraňování recyklovaných objektů se stará GC (*Garbage Collector*), jenž v pravidelných intervalech pročišťuje databázi **Active Directory**.

Doby životnosti smazaných a recyklovaných objektů lze kdykoliv změnit, doporučuje se ovšem nenastavovat tuto dobu kratší než 180 dnů. V případě obnovy smazaných **GPO** objektů nebo Exchange objektů platí omezení, že žádná aplikačně-specifická data pro tyto objekty, jenž nebyla uložena v databázi **Active Directory**, nebudou obnovena.

Od Windows Server 2012 je možné zapnout **Active Directory** Koš nejen pomocí **Powershellu**, ale také pohodlněji v **Active Directory Admninistrativ Center**.

Vztahy důvěry [Povinné]

V případě pracovní skupiny si každý počítač uchovává vlastní úložiště identit (*identity store*) ve formě **SAM** (*Security Accounts Manager*) databáze. Autentizace uživatelů probíhá oproti tomuto úložišti identit a pouze identity přítomné v tomto úložišti mohou mít definován přístup ke zdrojům na daném počítači. Pokud je počítač připojen do domény, vytvoří se vztah důvěry (*trust relationship*, *trust*) mezi tímto počítačem a doménou. Tento vztah důvěry způsobí, že uživatelé již nejsou autentizování lokálním systémem oproti lokálnímu úložišti identit, ale autentizačními službami domény (tedy **AD DS**) oproti doménovému úložišti identit (tedy databázi **Active Directory**). Připojený počítač také dovolí identitám z domény přistupovat k jeho lokálním zdrojům a využívat je.

Tento základní koncept lze samozřejmě rozšířit i na vztahy důvěry mezi jednotlivými doménami. Vztah důvěry mezi dvěma doménami umožňuje jedné doméně věřit autentizačním službám a úložišti identit druhé domény a používat identity z druhé domény k zabezpečení zdrojů. Každý vztah důvěry zahrnuje právě dvě domény, důvěřující (*trusting*) doménu a důvěryhodnou (*trusted*) doménu. Důvěryhodná doména obsahuje úložiště identit a poskytuje autentizační služby pro uživatele z tohoto úložiště. Pokud se uživatel z důvěryhodné domény přihlásí nebo připojí ke zdroji (počítači, souboru

[5] V případě čisté instalace lesa s funkční úrovní Windows Server 2008 R2 a vyšší již schéma obsahuje veškeré potřebné informace a není potřeba ho aktualizovat

atd.) v důvěřující doméně, nemůže být v této doméně autentizován, jelikož není přítomen v úložišti identit důvěřující domény. V tomto případě důvěřující doména přenechá autentizaci nějakému řadiči z důvěryhodné domény.

Protože důvěřující doména důvěřuje identitám z důvěryhodné domény, může důvěřující doména používat identity z důvěryhodné domény k zabezpečení svých vlastních zdrojů. Uživatelům z důvěryhodné domény lze přidělovat práva (*rights*) v důvěřující doméně, např. je možné uživatelům z důvěryhodné domény povolit přihlašovat se na počítače v důvěřující doméně. Uživatelé a globální skupiny z důvěryhodné domény mohou být také přidáni do doménově lokálních skupin v důvěřující doméně, případně i přímo do **ACL** seznamů jednotlivých zdrojů v důvěřující doméně.

Některé vztahy důvěry jsou vytvářeny automaticky, jiné musí být vytvořeny manuálně. V obou případech jsou ale tyto vztahy charakterizovány dvěma vlastnostmi:

- **Tranzitivita**. Vztahy důvěry mohou, nebo nemusí, být tranzitivní. Pokud doména **A** důvěřuje doméně **B** a doména **B** důvěřuje doméně **C** a oba tyto vztahy důvěry jsou tranzitivní, pak také doména **A** důvěřuje doméně **C**. V opačném případě, kdy některý ze vztahů není tranzitivní, to neplatí, doména **A** tedy nedůvěřuje doméně **C**.
- **Směr**. Vztahy důvěry mohou být jednosměrné (*one-way*) nebo obousměrné (*two-way*). V případě jednosměrného vztahu důvěry mohou uživatelé z důvěryhodné domény přistupovat ke zdrojům v důvěřující doméně, ovšem uživatelé z důvěřující domény nemohou přistupovat ke zdrojům v důvěryhodné doméně. U obousměrného vztahu důvěry mohou i uživatelé z důvěřující domény přistupovat ke zdrojům v důvěryhodné doméně.

V lese si všechny domény navzájem důvěřují. Přesněji kořenová doména každého doménového stromu v daném lese důvěřuje kořenové doméně lesa[6] a každá podřízená (*child*) doména důvěřuje své nadřízené (*parent*) doméně. Všechny tyto vztahy důvěry jsou tranzitivní a obousměrné. V konečném důsledku tedy každá doména důvěřuje všem ostatním.

Ostatní vztahy důvěry musí být vytvářeny manuálně. Existují celkem čtyři typy vztahů důvěry, jenž lze vytvořit manuálně:

- ***Shortcut***. Tento vztah důvěry se používá, pokud je potřeba urychlit přístup ke zdrojům nějaké domény z jiné domény ve stejném lese. Jak již bylo zmíněno výše, všechny domény v daném lese si navzájem důvěřuji, ovšem většinou jen nepřímo díky tranzitivitě vytvořených vztahů. Pokud se uživatel z jedné domény chce přihlásit na počítač v jiné doméně, musí proběhnout vyhodnocení všech tranzitivních vztahů po cestě do této cílové domény, kde se chce uživatel přihlásit, a ověřit tedy, že cílová doména důvěřuje výchozí doméně. Těchto vztahů ale může být mnoho a ověření tedy trvat příliš dlouho. *Shortcut* vztahy důvěry umožňují vytvořit vztah důvěry přímo mezi dvěma konkrétními podřízenými doménami. Díky tomu se důvěra mezi těmito doménami ověří jednoduše pomocí tohoto vztahu důvěry místo vyhodnocování všech vztahů důvěry po cestě z jedné domény do druhé. Tyto vztahy důvěry mohou být jednosměrné i obousměrné a jsou vždy tranzitivní, lze je tedy použít pro tvorbu nových, kratších, cest.
- ***External***. Tento vztah důvěry se používá, pokud je potřeba pracovat s doménami, jenž neleží ve stejném lese. Vytváří vztah důvěry mezi dvěma doménami systému Windows z odlišných lesů. Všechny tyto vztahy důvěry jsou jednosměrné a nejsou tranzitivní. Pokud je vytvořen obousměrný *external* vztah důvěry, jsou místo něj ve skutečnosti vytvořeny dva jednosměrné vztahy důvěry, každý v jednom směru. V případě, že je vytvořen odchozí *external* vztah důvěry, vytvoří **Active Directory** cizí (*foreign*) bezpečnostní objekt pro každý bezpečnostní objekt z důvěryhodné domény. Tyto cizí bezpečnostní objekty pak mohou být přidány do doménově lokálních skupin a ACL seznamů v důvěřující doméně. Pro zvýšení bezpečnosti tohoto vztahu důvěry lze využít výběrovou autentizaci a doménovou karanténu (povolena ve výchozím nastavení), které budou zmíněny dále.

[6] Kořenová doména lesa je první doména vytvořená v daném lese **Active Directory**

- ***Realm***. Tento vztah důvěry se používá, pokud je potřeba pracovat s bezpečnostními službami založenými na protokolu Kerberos v5, jenž běží na jiných systémech, než je systém Windows. Tyto vztahy důvěry jsou jednosměrné. Pro vytvoření obousměrného vztahu důvěry je možné vytvořit jednosměrné vztahy důvěry v každém z obou směrů. Ve výchozím nastavení nejsou tyto vztahy důvěry tranzitivní, ale lze je tranzitivními učinit.
- ***Forest***. Tento vztah důvěry se používá, pokud je potřeba spolupráce mezi dvěma organizacemi reprezentovanými pomocí dvou odlišných lesů. Vytváří vztah důvěry mezi kořenovými doménami obou lesů. Tyto vztahy mohou být jednosměrné i obousměrné a jsou vždy tranzitivní. Pokud existuje jednosměrný *forest* vztah důvěry mezi dvěma doménami, pak se uživatel z jakékoliv domény v důvěryhodném lese může přihlásit k jakémukoliv počítači v důvěřujícím lese (tedy k počítači v jakékoliv doméně v důvěřujícím lese). Pokud je tento vztah obousměrný, platí to i v opačném směru. *Forest* vztah důvěry má ve výchozím nastavení povolenou doménovou karanténu. Tento typ vztahů důvěry je vždy tranzitivní, ovšem pouze ve smyslu, že každá doména v důvěřujícím lese důvěřuje všem ostatním doménám v důvěryhodném lese. *Forest* vztahy důvěry nejsou tranzitivní navzájem. Tedy pokud les **A** důvěřuje lesu **B** a dále les **B** důvěřuje lesu **C**, pak neplatí, že les **A** důvěřuje lesu **C**. Aby bylo možné vytvořit *forest* vztah důvěry, je potřeba mít funkční úroveň lesa alespoň Windows Server 2003 a také mít odpovídající **DNS** infrastrukturu.

Zabezpečení vztahů důvěry

[Povinné]

Samotný vztah důvěry sice neumožňuje uživatelům přistupovat ke zdrojům v důvěřující doméně, ale jeho vytvořením mohou uživatelé z důvěryhodné domény získat přístup k některým zdrojům v důvěřující doméně. Je to proto, že velká řada zdrojů je chráněna ACL seznamy, které mohou mít definovány oprávnění pro skupinu Authenticated Users. Jelikož do této skupiny patří všichni autentizovaní uživatelé, tedy i autentizovaní uživatelé z důvěryhodných domén, mohou k těmto zdrojům přistupovat i tito uživatelé. Kromě toho mohou být samozřejmě uživatelé a globální skupiny z důvěryhodných domén přímo přidáni do ACL seznamů a také do doménově lokálních skupin.

I pokud jsou správně nastavena oprávnění pro přístup ke zdrojům v důvěřující doméně, je zde pořád nebezpečí nepovoleného přístupu. Když se uživatel autorizuje do důvěřující domény, předkládá autorizační data, jenž obsahují, mimo jiné, **SID** identifikátory uživatele a skupin, jichž je daný uživatel členem. Ne všechny tyto identifikátory musí pocházet (být vytvořeny) z důvěryhodné domény. Např. pokud je uživatel přesunut z jiné domény, je mu vygenerován nový **SID** identifikátor. V tomto případě ale uživatel ztrácí přístup ke zdrojům, jenž mají v ACL seznamech definovány oprávnění pro jeho starý **SID** identifikátor. Proto lze uchovávat u uživatele historii jeho předchozích **SID** identifikátorů. Ovšem tímto vzniká nebezpečí podstrčení **SID** identifikátorů. Administrátor může před migrací uživatele do nové domény přiřadit tomuto uživateli jako předchozí **SID** identifikátory **SID** identifikátory důležitých účtů z cílové domény (např. **SID** účtu, jenž je v Domain Admins) a uživatel tak získá díky historii oprávnění správce domény. Tento problém řeší doménová karanténa (*domain quarantine*), jenž zajišťuje ignorování veškerých **SID** identifikátorů, které nepocházejí z důvěryhodné domény. Doménová karanténa je ve výchozím nastavení povolena na všech *external* a *forest* vztazích důvěry.

Jak již bylo zmíněno dříve, autentizovaní uživatelé z důvěryhodné domény jsou automaticky členy Authenticated Users a mohou tedy mít automaticky přístup k řadě zdrojů v důvěřující doméně. Tato situace nemusí být vždy žádoucí. V případě přístupu ke zdrojům to lze řešit aplikací deny nebo odebráním oprávnění skupině Authenticated Users. Tímto postupem ale nelze omezit přístup ke službám jako je např. přihlašování ke stanicím v důvěřující doméně. Tento problém řeší výběrová autentizace (*selective authentication*), jenž umožňuje specifikovat, kteří uživatelé či skupiny mohou využívat služby na konkrétním počítači. Výběrovou autentizaci lze povolit u *external* a *forest* vztahů důvěry.

Lektorské úkoly

- Před spuštěním jednotlivých virtuálních strojů zkontrolujte správné nastavení jejich síťových adaptérů!!! U všech stanic (**w2012-dc**, **w2012-child** a **w2012-dc2**) musí být povoleny adaptéry *Internal* a *Private1*. A vždy v tomto pořadí!!!
- Na všech stanicích zakažte *Internal* síťové rozhraní (**Ethernet 1**) a povolte ho pouze v případech, že je potřeba přistupovat na externí síť!!!
- Pro přístup na server **yetti** přes *Internal* síťové rozhraní je nutné použít jeho plně kvalifikované doménové jméno **yetti.nepal.aps**

Lab L01 – Ochrana Active Directory [Na cvičeních]

Lab L02 – Záloha a obnova databáze Active Directory [Provést]

Cíl cvičení

Zálohovat a následně obnovit databázi **Active Directory**

Potřebné virtuální stroje

w2012-dc (D+R+C w2012-dc FIT)
w2012-child (D+R+C w2012-child FIT)

Další prerekvizity

Sdílený adresář **share** na **w2012-child**, do kterého může zapisovat uživatel **administrator**, Skupina **Simpsons** v doméně **testing.local**, účty uživatelů **homer** a **bart** v doméně **testing.local**

1. Přihlaste se na **w2012-dc** jako **testing\administrator**
2. Zálohujte databázi **Active Directory**
   a. Spusťte **Windows Server Backup**
      1. Start → Administrative Tools → **Windows Server Backup**
   b. V menu vyberte Action a zvolte Backup Once…
   c. V části Backup Options vyberte Different options a pokračujte Next >
   d. V další části Select Backup Configuration zvolte Custom a pokračujte Next >
   e. V následující části Select Items for Backup zvolte Add Items
   f. V seznamu věcí pro zálohování vyberte System state a potvrďte OK
   g. Pokračujte Next >
   h. V části Specify Destination Type zvolte Remote shared folder a pokračujte Next >
   i. V další části Specify Remote Folder zadejte u Location adresář **\\w2012-child\share**, pod Access Control ponechte Inherit a pokračujte Next >
   j. Proveďte zálohu stavu systému pomocí Backup
      - Zálohu **neprovádějte**, je již předpřipravena v **\\w2012-child\share**
   k. Po dokončení zálohování uzavřete průvodce pomocí Close
3. Smažte skupinu **Simpsons** a uživatele **homer** a **bart**
4. Proveďte autoritativní obnovu databáze Active Directory
   a. Restartujte **w2012-dc** v **DSRM** (*Directory Services Restore Mode*) režimu
      1. Z příkazové řádky spusťte **shutdown –o –r**

2. Systém se po krátké chvíli restartuje a následně ukáže nabídku se základními možnostmi spuštění
3. V nabídce zvolte Troubleshoot – Startup Settings a potvrďte tlačítkem Restart
   - Po restartu se yobrayí nabídka **Advanced Boot Options**
   - Na starších verzích Windows lze tuto nabídku vyvolat klávesou **F8** na začátku bootování systému Windows
4. Vyberte **Directory Services Restore Mode**
5. Přihlaste se lokálně jako uživatel **administrator**, heslo **aaa**
   - **w2012-dc\administrator** nebo **.\administrator**

b. Spusťte **Windows Server Backup**
   1. Start → Administrative Tools → **Windows Server Backup**

c. V levém sloupci vyberte uzel Local Backup
d. V menu vyberte Action a zvolte Recover…
e. V části Getting Started vyberte A backup stored on another location a pokračujte Next >
f. V další části Specify Location Type zvolte Remote shared folder a pokračujte Next >
g. V následující části Specify Remote Folder zadejte adresář **\\w2012-child\share** a pak pokračujte Next >
h. V části Select Backup Date zvolte datum a čas poslední zálohy a pokračujte Next >
i. V další části Select Recovery Type zvolte System State a pokračujte Next >
j. V následující části Select Location for System State Recovery ponechte Original Location, zaškrtněte Perform an authoritative restore of Active Directory files a pokračujte Next >
k. Potvrďte dvakrát OK
l. Zahajte autoritativní obnovu pomocí Recover a potvrďte Yes
   - Obnovu neprovádějte, vraťte se zpět do části Select Recovery Type obnovte pouze databázi **Active Directory** (soubor **C:\Windows\NTDS\ntds.dit**)

5. Restartujte **w2012-dc** a zkontrolujte, že byly obnoveny objekty smazané v bodě 3

Lab L03 – ADDT (Active Directory Domains and Trusts) [Na cvičeních]

Lab L04 – Vytvoření vztahů důvěry [Provést]

Cíl cvičení

Vytvořit postupně *external* a *forest* vztahy důvěry, ověřit jejich funkčnost a seznámit se s jejich odlišnostmi při vyhodnocování důvěry mezi doménami

Potřebné virtuální stroje

w2012-dc (D+R+C w2012-dc FIT)
w2012-child (D+R+C w2012-child FIT)
w2012-dc2 (w2012-dc2 FIT)

Další prerekvizity

Účet uživatele **administrator** v doméně **testing2.local2**

1. Nastavte podmíněné přeposílání DNS dotazů mezi doménami **testing.local** a **testing2.local2**
   a. Na **w2012-dc** otevřete **DNS**
      1. Start → Administrative Tools → **DNS**
   b. Klikněte pravým na Conditional Forwarders a zvolte New Conditional Forwarder…

c. Do pole DNS Domain zadejte **testing2.local2** a pod IP addresses of the master servers níže vložte IP adresu **192.168.50.90** a potvrďte OK
d. Opakujte **body 1.a – 1.c** na **w2012-dc2**, tentokrát pro doménu **testing.local** a IP adresu **192.168.50.5**

2. Vytvořte nový *external* vztah důvěry tak, aby doména **child.testing.local** důvěřovala doméně **testing2.local2**
   a. Na **w2012-dc** otevřete **ADDT** (*Active Directory Domains and Trusts*)
      1. Start → Administrative Tools → **Active Directory Domains and Trusts**
   b. Klikněte pravým na doménu **child.testing.local** a zvolte Properties
   c. Přejděte na záložku Trusts a zvolte New Trust…
   d. V průvodci pokračujte Next >
   e. V části Trust Name zadejte do pole Name doménu **testing2.local2** a pokračujte Next >
   f. V další části Direction of Trust zvolte One way: outgoing a pokračujte Next >
   g. V následující části Sides of Trust zvolte Both this domain and the specified domain a pak pokračujte Next >
   h. V další části User Name and Password zadejte účet uživatele **administrator** a heslo **aaa** a pokračujte Next >
   i. V části Outgoing Trust Authentication Level – Local Domain zvolte možnost Domain-wide authentication a pokračujte Next >
   j. Vytvořte nový vztah důvěry pomocí Next >
   k. Pokračujte Next >
   l. V části Confirm Outgoing Trust zvolte Yes, confirm the outgoing trust a pokračujte Next >
   m. Potvrďte pomocí Finish
3. Povolte všem uživatelům přihlásit se na řadiče domény v doméně **child.testing.local**
   a. Na **w2012-child** otevřete **GPME** (*Group Policy Management Editor*)
      1. Start → Administrative Tools → **Group Policy Management**
   b. Klikněte pravým na GPO objekt Default Domain Controllers Policy a zvolte Edit…
   c. Vyberte uzel Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Local Policies \ User Rights Assignments
   d. Klikněte pravým na Allow log on locally a zvolte Properties
   e. Zaškrtněte Define these policy settings a zvolte Add User or Group…
   f. Zadejte **Everyone** a potvrďte OK
   g. Potvrďte OK a zavřete Group Policy Management Editor
   h. Aktualizujte nastavení zásad skupiny příkazem **gpupdate /force**
4. Přihlaste se na **w2012-child** jako uživatel **administrator@testing2.local2**
   - Přihlášení bude úspěšné, jelikož doména **testing2.local2** je důvěryhodnou doménou pro doménu **child.testing.local**
5. Povolte všem uživatelům přihlásit se na řadiče domény v doméně **testing2.local2** provedením postupu z **bodu 3** na **w2012-dc2**
6. Přihlaste se na **w2012-dc2** jako uživatel **administrator@child.testing.local**
   - Přihlášení nebude úspěšné, jelikož doména **child.testing.local** není důvěryhodnou doménou pro doménu **testing2.local2**, vytvořený vztah je jednosměrný
7. Povolte všem uživatelům přihlásit se na řadiče domény v doméně **testing.local** provedením postupu **bodu 3** na **w2012-dc**

8. Přihlaste se na **w2012-dc** jako uživatel **administrator@testing2.local2**
   - Přihlášení nebude úspěšné, jelikož doména **testing2.local2** není důvěryhodnou doménou pro doménu **testing.local**
9. Smažte vytvořený *external* vztah důvěry mezi doménami **child.testing.local** a **testing2.local2**
   a. Na **w2012-dc** otevřete **ADDT** (*Active Directory Domains and Trusts*)
      1. Start → Administrative Tools → **Active Directory Domains and Trusts**
   b. Klikněte pravým na doménu **child.testing.local** a zvolte Properties
   c. Přejděte na záložku Trusts
   d. Pod Domains trusted by this domain (outgoing trusts) vyberte v seznamu **testing2.local2** zvolte Remove
   e. Vyberte Yes, remove the trust from both the local domain and the other domain a použijte účet uživatele **administrator** s heslem **aaa**
   f. Potvrďte odebrání pomocí Yes
10. Vytvořte *forest* vztah důvěry tak, aby kořenová doména lesa **testing.local** důvěřovala kořenové doméně lesa **testing2.local2**
    a. Na **w2012-dc** otevřete **ADDT** (*Active Directory Domains and Trusts*)
       1. Start → Administrative Tools → **Active Directory Domains and Trusts**
    b. Klikněte pravým na doménu **testing.local** a zvolte Properties
    c. Přejděte na záložku Trusts a zvolte New Trust…
    d. V průvodci pokračujte Next >
    e. V části Trust Name zadejte do pole Name doménu **testing2.local2** a pokračujte Next >
    f. V další části Trust Type vyberte Forest Trust a pokračujte Next >
    g. V následující části Direction of Trust zvolte One way: outgoing a pokračujte Next >
    h. V části Sides of Trust ponechte This domain only a pokračujte Next >
    i. V další části Outgoing Trust Authentication Level zvolte Forest-wide authentication a pokračujte Next >
    j. V následující části Trust Password použijte heslo **aaaAAA111** a pokračujte Next >
    k. Vytvořte nový vztah důvěry pomocí Next >
    l. Pokračujete Next >
    m. V části Confirm Outgoing Trust zvolte No, do not confirm the outgoing trust a pokračujte Next >
    n. Potvrďte pomocí Finish
11. Dokončete vytvoření forest vztahu důvěry v doméně **testing2.local2**
    a. Na **w2012-dc2** otevřete **ADDT** (*Active Directory Domains and Trusts*)
       1. Start → Administrative Tools → **Active Directory Domains and Trusts**
    b. Klikněte pravým na doménu **testing2.local2** a zvolte Properties
    c. Přejděte na záložku Trusts a zvolte New Trust…
    d. V průvodci pokračujte Next >
    e. V části Trust Name zadejte do pole Name doménu testing.local a pokračujte Next >
    f. V další části Trust Type vyberte Forest Trust a pokračujte Next >
    g. V následující části Direction of Trust zvolte One way: incoming a pokračujte Next >
    h. V části Sides of Trust ponechte This domain only a pokračujte Next >
    i. V další části Trust Password zadejte heslo **aaaAAA111** a pokračujte Next >
    j. Vytvořte nový vztah důvěry pomocí Next >
    k. Pokračujte Next >

l. V části Confirm Incoming Trust zvolte Yes, confirm the incoming trust a zadejte účet uživatele **administrator** a heslo **aaa** a pokračujte Next >
m. Potvrďte pomocí Finish

12. Přihlaste se na **w2012-dc** jako uživatel **administrator@testing2.local2**
    - Přihlášení bude úspěšné, jelikož doména **testing2.local2** je důvěryhodnou doménou pro doménu **testing.local**
13. Přihlaste se na **w2012-dc2** jako uživatel **administrator@testing.local**
    - Přihlášení nebude úspěšné, jelikož doména **testing.local** není důvěryhodnou doménou pro doménu **testing2.local2**, vytvořený vztah je jednosměrný
14. Přihlaste se na **w2012-child** jako uživatel **administrator@testing2.local2**
    - Přihlášení bude úspěšné, jelikož doména **testing2.local2** je důvěryhodnou doménou pro doménu **testing.local**, doména **child.testing.local** důvěřuje své nadřízené (*parent*) doméně **testing.local**, doména **testing.local** zase důvěřuje **testing2.local2** doméně, oba tyto vztahy důvěry jsou tranzitivní, takže také doména **child.testing.local** důvěřuje doméně **testing2.local2**

Studentské úkoly

- Na všech stanicích zakažte *Internal* síťové rozhraní (**Ethernet 1**) a povolte ho pouze v případech, že je potřeba přistupovat na externí síť!!!

Lab S01 – Obnova objektů

[Povinné]

Cíl cvičení

Obnovit smazané objekty bez a s přítomností **Active Directory** koše

Potřebné virtuální stroje

w2012-dc (D+R+C w2012-dc FIT)

Další prerekvizity

Účty uživatelů **bart** a **homer** v doméně **testing.local**, jenž jsou členy skupiny **Simpsons**

1. Vymažte účet uživatele **bart**
   - Objekt se stane tzv. *tombstoned* objektem
2. Obnovte účet uživatele **bart**
   a. Spusťte nástroj **ldp.exe**
   b. V menu vyberte Connection a pak zvolte Connect…
   c. Do pole Server zadejte **w2012-dc.testing.local** a připojte se pomocí OK
   d. V menu opět vyberte Connection a zvolte Bind…
   e. Pod Bind type zvolte Bind as currently logged on user a potvrďte OK
   f. V menu vyberte Options a zvolte Controls
   g. Pod Control Type zvolte Server a pak v Load Predefined seznamu vyberte Return deleted objects, potvrďte OK
   h. V menu vyberte View a zvolte Tree
   i. Po pole BaseDN zadejte **cn=Deleted Objects,dc=testing,dc=local** a potvrďte OK
   j. Lokalizujte účet uživatele **bart**, klikněte na něj pravým a zvolte Modify
      - Účet bude začínat **cn=bart\0ADEL…**
   k. Do pole Edit Entry Attribute zadejte **isDeleted**, jako Operation zvolte Delete a potvrďte pomocí Enter
   l. Do pole Edit Entry Attribute zadejte **distinguishedName**, do pole Value zadejte **cn=bart, cn=Users,dc=testing,dc=local**, jako Operation zvolte Replace a potvrďte pomocí Enter
   m. Zaškrtněte možnosti Synchronous a Extended níže a proveďte příkaz pomocí Run
3. Ověřte, že byl účet uživatele **bart** skutečně obnoven
   - Uživatel **bart** nebude členem skupiny **Simpsons**, jelikož se tato informace u *tombstoned* objektů neuchovává, stejně jako hodnoty řady dalších atributů
   - Všimněte si, že je účet **zakázán** (*disabled*)
4. Povolte **Active Directory** koš
   - Pozor, jakmile je **Active Directory** koš povolen, nelze již zpět zakázat
   a. Pomocí **ADAC** (*Active Directory Administrative Center*)
      1. Otevřete **ADAC**
         a. Start → Administrative Tools → **Active Directory Administrative Center**
      2. V navigačním panelu (vlevo) zvolte **testing (local)**

3. V panelu úkolů (vpravo), nebo z kontextové nabídky zvolte Enable Recycle Bin … a 2x potvrďte OK
   - ➢ Aby se změna projevila i v konzoli **ADAC**, je vhodné ji ukončit a opět otevřít

b. Pomocí **Powershellu** (lze i ve Windows 2008R2)
   1. Spusťte jako administrátor **Active Directory Module for Windows PowerShell**
      a. Start → **Administrative Tools**
      b. Klikněte pravým na **Active Directory Module for Windows PowerShell** a zvolte Run as administrator
   2. Spusťte příkaz **Enable-ADOptionalFeature -Identity "CN=Recycle Bin Feature, CN=Optional Features, CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration, DC=testing, DC=local" -Scope ForestOrConfigurationSet -Target "testing.local"**
   3. Potvrďte pomocí **Y**

2. Vymažte účet uživatele **homer**
   - ➢ Objekt se stane smazaným objektem, nový stav u **Active Directory** koše
3. Obnovte účet uživatele **homer**
   a. Pomocí **ADAC** (*Active Directory Administrative Center*)
      1. Otevřete **ADAC**
         a. Start → Administrative Tools → **Active Directory Administrative Center**
      2. V navigačním panelu (vlevo) zvolte **testing (local)** – **Deleted Objects**
      3. Vyberte účet **Homer** a z panelu úkolů (nebo kontextové nabídky) zvolte Restore
      - ➢ Alternativně lze použít Restore To … pro obnovené do jiného umístění

   b. Pomocí **Powershellu**
      1. Spusťte jako administrátor **Active Directory Module for Windows PowerShell**
      2. Spusťte příkaz **Get-ADObject -Filter {sAMAccountName -eq "homer"} -IncludeDeletedObjects | Restore-ADObject**
      - ➢ Objekt lze obnovit také postupem z **bodu** Chyba! Nenalezen zdroj odkazů.
4. Ověřte, že byl účet uživatele **homer** skutečně obnoven
   - ➢ Uživatel **homer** bude pořád členem skupiny **Simpsons**, jelikož **Active Directory** koš uchovává veškeré informace (přímé i nepřímé) u smazaných objektů

Lab S02 – Zabezpečení vztahů důvěry

[Povinné]

Cíl cvičení

Nastavit a ověřit výběrovou autentizaci, vypnout a zapnout doménovou karanténu

Potřebné virtuální stroje

w2012-dc (D+R+C w2012-dc FIT)
w2012-child (D+R+C w2012-child FIT)
w2012-dc2 (w2012-dc2 FIT)

Další prerekvizity

Dokončený úkol **Lab L04**

1. Povolte výběrovou autentizaci pro *forest* vztah důvěry mezi **testing.local** a **testing2.local2**
   a. Na **w2012-dc** otevřete **ADDT** (*Active Directory Domains and Trusts*)
      1. Start → Administrative Tools → **Active Directory Domains and Trusts**

b. Klikněte pravým na doménu **testing.local** a zvolte Properties
c. Přejděte na záložku Trusts
d. Pod Domains trusted by this domain (outgoing trusts) vyberte v seznamu **testing2.local2** zvolte Properties…
e. Přejděte na záložku Authentication a vyberte Selective authentication
f. Potvrďte dvakrát OK

2. Přihlaste se na **w2012-dc** jako uživatel **administrator@testing2.local2**
   - Přihlášení nebude úspěšné, jelikož po povolení selektivní *autentizace* nelze využívat žádné služby počítačů v důvěřující doméně
3. Povolte využívání služeb **w2012-dc**
   a. Na **w2012-dc** otevřete **ADUC** (*Active Directory Users and Computers*)
      1. Start → Administrative Tools → **Active Directory Users and Computers**
   b. Povolte pokročilé možnosti zobrazení
      1. V menu konzole vyberte View a zvolte Advanced Features
   c. Vyberte organizační jednotku Domain Controllers
   d. Klikněte pravým na účet počítače **w2012-dc** a zvolte Properties
   e. Přejděte na záložku Security, pak v seznamu pod Group or user names vyberte skupinu Authenticated Users a zaškrtněte Allow u Allowed to authenticate
   f. Potvrďte OK
4. Přihlaste se na **w2012-dc** jako uživatel **administrator@testing2.local2**
   - Přihlášení již bude úspěšné, jelikož všichni uživatelé z důvěryhodných domén jsou členy skupiny Authenticated Users a ta má nyní oprávnění využívat služby tohoto počítače
5. Vypněte doménovou karanténu pro *forest* vztah důvěry mezi **testing.local** a **testing2.local2**
   a. Na **w2012-dc** spusťte jako administrátor příkazový řádek
   b. Spusťte příkaz **netdom trust testing.local /d:testing2.local2 /quarantine:no /userD:administrator@testing2.local2 /passwordD:aaa**
6. Zapněte doménovou karanténu pro *forest* vztah důvěry mezi **testing.local** a **testing2.local2**
   a. Na **w2012-dc** spusťte jako administrátor příkazový řádek
   b. Spusťte příkaz **netdom trust testing.local /d:testing2.local2 /quarantine:yes /userD:administrator@testing2.local2 /passwordD:aaa**

Lab S03 – Snímky databáze Active Directory

[Volitelné]

Cíl cvičení

Vytvořit snímek databáze Active Directory a zobrazit ho

Potřebné virtuální stroje

w2012-dc (D+R+C w2012-dc FIT)

Další prerekvizity

Účet uživatele **bart** v doméně **testing.local**

1. Vytvořte snímek aktuálního stavu databáze **Active Directory**
   a. Spusťte jako administrátor příkazovou řádku
   b. Spusťte nástroj **ntdsutil**
   c. Vyberte databázi **Active Directory** příkazem **activate instance NTDS**

d. Přejděte do správy snímků příkazem **snapshot**
e. Vytvořte nový snímek příkazem **create**
   - Snímky se také vytvářejí automaticky pří záloze databáze **Active Directory**

2. Proveďte nějakou změnu v databázi **Active Directory** u uživatele **bart**, např. změňte hodnotu atributu Description
3. Vytvořte LDAP server obsahující dříve vytvořený snímek databáze **Active Directory**
   a. Ve správě snímků (snapshot:) v nástroji **ntdsutil** zobrazte seznam všech snímků příkazem **list all**
      - Seznam obsahuje všechny dostupné snímky (manuálně vytvořené či obsažené v zálohách), každý řádek seznamu odpovídá jednomu snímku a je ve formátu **<index>: <popis> {<guid>}**, kde **<popis>** může být datum a čas pořízení snímku (zálohy) nebo umístění
   b. Připojte snímek příkazem **mount <index>**, případně **mount <guid>**
      - Použijte **<index>** nebo **<guid>** posledního snímku ze seznamu snímků, po připojení bude vypsána cesta k připojenému snímku
   c. Spusťte jako administrátor druhý příkazový řádek
   d. Spusťte příkaz **dsamain -dbpath <cesta ke snímku> -ldapport 65000**
      - Jako cestu ke snímku použijte cestu vrácenou při připojování snímku, měla by být ve formátu **C:\$SNAP_<datum a čas>_VOLUMEC$\Windows\NTDS\ntds.dit**
      - Zvolený port musí být možné použít, tedy nesmí být již využíván jinou aplikací, nesmí být blokován či rezervován (systémem nebo jinak), doporučuje se používat čísla vyšší než **50000**, které lze většinou použít
4. Zobrazte obsah vytvořeného snímku databáze **Active Directory**
   a. Otevřete **ADUC** (*Active Directory Users and Computers*)
      1. Start → Administrative Tools → **Active Directory Users and Computers**
   b. Klikněte pravým na uzel Active Directory Users and Computers a zvolte Change Domain Controller…
   c. Pod Change to zvolte možnost This Domain Controller or AD LDS instance a níže zadejte **w2012-dc:65000**
      - Pokud bude místo hostitelského jména LDAP serveru zadána jeho IP adresa, nebude možné se k tomuto serveru připojit
   d. Potvrďte OK
5. Ověřte, že snímek neobsahuje změny provedené u uživatele **bart** po vytvoření snímku

Lab S04 – Auditování změn databáze Active Directory

[Volitelné]

Cíl cvičení

Povolit a ověřit auditování změn v databázi Active Directory

Potřebné virtuální stroje

w2012-dc (D+R+C w2012-dc FIT)

Další prerekvizity

Účet uživatele **bart** v doméně **testing.local**

1. Povolte auditování změn v databázi **Active Directory**
   a. Otevřete **GPME** (*Group Policy Management Editor*)

1. Start → Administrative Tools → **Group Policy Management**

b. Klikněte pravým na GPO objekt Default Domain Controllers Policy a zvolte Edit…
c. Vyberte uzel Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Advanced Audit Policy Configuration \ Audit Policies \ DS Access
d. Klikněte pravým na Audit Directory Service Changes a zvolte Properties
e. Zaškrtněte Configure the following audit events, pak Success a potvrďte OK
   - Toto nastavení zajistí auditování úspěšných změn v databázi **Active Directory**
f. Vyberte uzel Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Local Policies \ Security Options
g. Klikněte pravým na Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings a zvolte Properties
h. Zaškrtněte Define these policy settings a zvolte Enabled a potvrďte OK
   - Toto nastavení zapíná pokročilé zásady auditování, pokud není tato zásada povolena, ignorují počítače nastavení auditování, jenž jsou obsažená pod uzlem Advanced Audit Policy Configuration
i. Zavřete Group Policy Management Editor
j. Aktualizujte nastavení zásad skupiny příkazem **gpupdate /force**

2. Ověřte, že auditování změn v databázi **Active Directory** bylo povoleno
   a. Spusťte příkazovou řádku
   b. Spusťte příkaz **auditpol.exe /get /category:"DS Access"**
   c. Ověřte, že u podkategorie Directory Service Changes je nastavení **Success**
3. Přidejte uživatele **bart** do skupiny Domain Admins
   - Obecně nedochází k auditování veškerých změn v databázi **Active Directory**, zazmenávají se pouze důležitější změny, např. změny členství ve skupinách
4. Ověřte zaznamenání přidání uživatele **bart** do skupiny Domain Admins
   a. Otevřete **Event Viewer**
      1. Start → Administrative Tools → **Event Viewer**
   b. Vyberte uzel Windows Logs \ Security
   c. Lokalizujte a vyberte poslední událost s Event ID **5136**
   d. Na záložce Details ověřte, že zaznamenána událost se týká členství ve skupině Domain Admins (hodnota ObjectDN je **CN=Domain Admins,CN=Users,DC=testing,DC=local**), že došlo ke změně členů této skupiny, neboli že došlo k modifikaci atributu member (hodnota AttributeLDAPDisplayName je **member**), a také že byt přidán uživatel **bart** (hodnota AttributeValue je **CN=bart,CN=Users,DC=testing,DC=local** a hodnota OperationType je **%%14674**)

Lab S05 – Údržba databáze Active Directory

[Volitelné]

Cíl cvičení

Provést údržbu databáze Active Directory

Potřebné virtuální stroje

w2012-dc (D+R+C w2012-dc FIT)

Další prerekvizity

Adresář **C:\share**

1. Vypněte doménové služby **Active Directory** (**AD DS**)
   a. Otevřete konzoli **Services**
      1. Start → Administrative Tools → **Services**
   b. Klikněte pravým na Active Directory Domain Services a zvolte Stop
   c. Potvrďte zastavení ostatních souvisejících služeb pomocí Yes
2. Proveďte zkompaktnění databáze **Active Directory**
   a. Spusťte jako administrátor příkazovou řádku
   b. Spusťte nástroj **ntdsutil**
   c. Vyberte databázi **Active Directory** příkazem **activate instance NTDS**
   d. Přejděte do údržby souborů příkazem **files**
   e. Proveďte *zkompaktnění* databáze příkazem **compact to C:\share**
      - Při *zkompaktňování* se vytváří nová databáze **Active Directory**, která již neobsahuje dříve alokované nepotřebné místo
   f. Ukončete nástroj **ntdsutil** příkazy **quit** a **quit**
3. Nahraďte starou databázi **Active Directory** její *zkompaktněnou formou*
   a. Smažte staré protokoly příkazem **del C:\Windows\NTDS*.log**
   b. Nahraďte databázi příkazem **copy "C:\share\ntds.dit" "C:\Windows\NTDS\ntds.dit"**
   c. Potvrďte přepsání databáze pomocí **Yes**
4. Ověřte integritu a sémantiku nové databáze **Active Directory**
   a. Spusťte nástroj **ntdsutil**
   b. Vyberte databázi **Active Directory** příkazem **activate instance NTDS**
   c. Přejděte do údržby souborů příkazem **files**
   d. Spusťte kontrolu integrity databáze příkazem **integrity**
   e. Vraťte se zpět příkazem **quit**
   f. Přejděte do části ověřování sémantiky databáze příkazem **semantic database analysis**
   g. Ověřte sémantiku databáze příkazem **go fixup**
   h. Ukončete nástroj **ntdsutil** příkazy **quit** a **quit**
5. Zapněte doménové služby **Active Directory** (**AD DS**)
   a. Otevřete konzoli **Services**
      1. Start → Administrative Tools → **Services**
   b. Klikněte pravým na Active Directory Domain Services a zvolte Start