RODC (Read-Only Domain Controller) [Povinné]

Pokud je nějaká doména rozprostřena přes více míst (*sites*), nastává otázka, kde umístit jednotlivé řadiče domény. Síťová propojení mezi místy nejčastěji vytvářejí hvězdicovou topologii, existuje tedy jedno hlavní místo (*hub site*, *main office*), jenž je spojeno se všemi ostatními vedlejšími místy (*branch office*). Obecně lze říci, že vedlejší místa nikdy nedosahují takové úrovně zabezpečení, jakou má místo hlavní. Spojení mezi hlavním a vedlejším místem bývá pomalé, což vede často k jeho zahlcení, nebo nespolehlivé, kdy může docházet k častým výpadkům. Nakonec, vedlejší místa mívají velice omezený personál pro správu řadičů domény a techniky obecně.

Asi nejlepším řešením by bylo umístit všechny řadiče domény do hlavního místa. Tento postup ale vede k několika problémům:

- **Autentizace**. Zde je dobré rozlišovat dva typy *autentizace* – do domény a ke službám. V obou případech musí *autentizaci* provést řadič domény, jenž se nachází v hlavním místě. Tedy tato *autentizace* probíhá přes (potenciálně pomalé) spojení mezi vedlejším a hlavním místem. Pokud je toto spojení přerušeno, nemůže se uživatel přihlásit. Jelikož se ale uživatel přihlašuje většinou jen jednou denně, není tento typ *autentizace* až tak kritický. V případě *autentizace* ke službám se využívá tzv. *service tickets*, jakýchsi klíčů, jenž umožňují uživateli přistupovat ke specifickým službám. Tyto klíče vydávají řadiče domény jednotlivým uživatelům. Protože uživatel často využívá více služeb během jednoho dne, je pro tento typ *autentizace* nezbytné mít rychlé a spolehlivé spojení s řadičem domény v hlavním místě.
- **Vyhledávání**. K vyhledávání informací v doméně je potřeba globální katalog. Všechny dotazy musí být tedy přeposílány řadičům domény v hlavním místě, které nesou globální katalog. To vede k dalšímu zahlcování spojení a pomalému vyhledávání.

Nasazení řadičů domény do vedlejších míst sice vyřeší výše zmíněné problémy, ale za cenu vytvoření problémů nových:

- **Správa**. V případě údržby řadiče domény (např. instalace ovladače pro nový hardware) je potřeba se na něj přihlásit jako lokální správce (člen skupiny Administrators). Ovšem na řadičích domény jsou všichni lokální správci zároveň také správci domény (členové Domain Admins) a mohou tedy spravovat celou doménu. Většinou není vhodné, aby lokální správci ve vedlejším místě měli takovéto možnosti, jelikož to zvyšuje nebezpečí výskytu problémů popsaných níže.
- **Konzistence**. Veškeré změny v **Active Directory** databázi na řadiči domény ve vedlejším místě jsou replikovány na ostatní řadiče domény. Poškození databáze může vážně narušit integritu doménových služeb, jelikož chybná data mohou být replikována do celé domény.
- **Bezpečnost**. Každý řadič domény uchovává kopii veškerých informací o všech objektech v doméně, včetně tajných informací jako uživatelských hesel. V případě nepovoleného přístupu či odcizení řadiče domény je možné tyto informace získat.

RODC řadiče jsou speciální řadiče domény určené primárně pro nasazení do vedlejších míst. Každý **RODC** řadič obsahuje kopii veškerých objektů domény a jejich atributů, stejně jako každý normální řadič domény, s výjimkou atributů obsahujících tajné informace, jako jsou hesla. **RODC** řadič tedy nemůže provádět *autentizaci*. Lze ale nastavit zásadu replikace hesel (PRP, *Password Replication Policy*), která umožňuje specifikovat uživatele, jejichž účty bude **RODC** řadič uchovávat ve své vyrovnávací paměti (*kešovat*). Pokud se takovýto uživatel přihlásí, uloží **RODC** řadič jeho pověření[1] (*credentials*) do své vyrovnávací paměti. Při příštím přihlašování tohoto uživatele použije **RODC** řadič informace uložené v této paměti namísto toho, aby žádost o přihlášení přeposlal k vyřízení normálnímu řadiči domény. Navíc si normální řadiče domény uchovávají informace o tom, která pověření jsou přítomna ve vyrovnávacích pamětech jednotlivých **RODC** řadičů. V případě, že dojde k odcizení

[1] Pověření je sada informací sloužící k *autentizaci* určité entity (uživatele, počítače apod.), v případě uživatele to jsou nejčastěji informace o uživatelském jméně a hesle

nějakého **RODC** řadiče a je potřeba nastavit nová hesla pro uživatele, jejichž účty byly *kešovány*, jsou tyto informace k dispozici. Přesněji, při odstranění účtu **RODC** řadiče z **Active Directory** systém automaticky nabídne možnost provést *reset* uživatelských hesel pro *kešované* účty.

Kopie **Active Directory** databáze, kterou obsahují **RODC** řadiče je určena pouze pro čtení, nelze do ní tedy přímo zapisovat. Pokud nějaká aplikace potřebuje číst z **Active Directory**, zpracuje **RODC** řadič tento požadavek a povolí jí přístup. V případě zápisu je aplikace přesměrována na normální řadič domény, který provede požadované změny v **Active Directory** databázi. Tyto změny jsou pak replikovány na ostatní řadiče domény, včetně **RODC** řadičů. Replikace je z pohledu **RODC** řadičů jednosměrná, probíhá vždy pouze z normálních řadičů domény na **RODC** řadiče, nikdy opačně. To zabraňuje situaci, že dojde k replikaci podvržených či poškozených dat v **Active Directory** databázi a také redukuje zátěž tzv. *bridgehead* serverů (viz pozdější sekce). Jednosměrná replikace se týká také adresáře **SYSVOL**. Do tohoto adresáře mohou sice **RODC** řadiče zapisovat, ale stejně jako v případě **Active Directory** databáze nebudou tyto změny replikovány na ostatní řadiče domény.

U **RODC** řadičů může být funkce lokálního administrátora delegována jakémukoliv doménovému uživateli nebo bezpečnostní skupině (*security group*). Takto pověření uživatelé se mohou přihlásit na daný **RODC** řadič a provádět akce spojené s údržbou, aniž by zároveň získali nadměrná oprávnění pro akce v rámci domény. Tito uživatelé se také nemohou přihlásit na žádný jiný řadič domény.

RODC řadiče mohou samozřejmě plnit úlohu **DNS** serveru. V případě, že je spravovaná zóna integrována do databáze **Active Directory** jsou zde ale rozdíly. Stejně jako celá databáze **Active Directory** i v ní integrované zóny jsou určeny pouze pro čtení. Tyto zóny lze považovat za obdobu sekundárních zón u systému **DNS**. Jediná možnost jak změnit obsah takovéto zóny je skrz replikaci. Díky tomu také **RODC** řadiče nepodporují dynamické aktualizace **DNS** záznamů klienty, které musí probíhat nepřímo. Pokud se klient pokusí aktualizovat svůj **DNS** záznam u **RODC** řadiče, vrátí mu řadič odkaz na jiný **DNS** server. Klient pak zkusí aktualizovat svůj záznam u tohoto **DNS** serveru. Zároveň se **RODC** řadič pokusí replikovat klientem aktualizovaný záznam z tohoto **DNS** serveru. Tato replikace je ovšem speciální, týká se pouze jediného objektu, pouze aktualizovaného záznamu. Ostatní změny nejsou replikovány.

I přesto, že **RODC** řadiče mohou plnit různé role, nemohou být nikdy operačními servery. Mohou ovšem nést globální katalog, což je důležité pro vyhledávání.

Instalace

[Povinné]

Než je možné povýšit nějaký server do role **RODC** řadiče, je nejprve potřeba ověřit splnění několika podmínek a případně připravit daný les na nasazení **RODC** řadičů. Proces instalace **RODC** řadičů se dá rozdělit na tři části:

- **Ověření požadavků**. Nasazení **RODC** řadičů vyžaduje, aby funkční úroveň lesa byla minimálně Windows Server 2003. Je tedy potřeba ověřit, že na všech řadičích domény v daném lese běží systém Windows Server 2003. Pak zkontrolovat funkční úroveň všech domén v daném lese a případně ji zvýšit na úroveň Windows Server 2003. Potom už jen zbývá ověřit funkční úroveň samotného lesa. Druhým požadavkem je existence minimálně jednoho normálního řadiče domény v dané doméně, na němž běží alespoň Windows Server 2008. **RODC** řadiče totiž mohou replikovat doménová data[2] jen z takovýchto řadičů domény, nelze je nikdy replikovat z jiných **RODC** řadičů ani z normálních řadičů domény, na nichž běží Windows Server 2003 nebo starší systém. Pokud **RODC** řadič plní i úlohu **DNS** serveru, musí nějaký z řadičů domény, na kterých běží Windows Server 2008 a novější, také obsahovat danou **DNS** zónu.
- **Příprava lesa**. Protože **RODC** řadiče mohou být nainstalovány jen na počítače, na kterých běží Windows Server 2008 nebo novější, musí být možné přidat počítače s tímto systémem do existujícího lesa. V případě existujícího lesa (s funkční úrovní Windows Server 2003 a nižší), je

[2] Doménovými daty rozumíme veškerá data, jež podléhají replikaci z hlediska **Active Directory**, nejsou to tedy jen data z databáze **Active Directory**, ale např. i data z adresáře **SYSVOL** apod.

nutné připravit tento les pomocí **adpred /forestprep** a následně umožnit existenci **RODC** řadičů v doménách pomocí **adprep /rodcprep**. Tyto příkazy slouží k aktualizaci schématu daného lesa.

- **Instalace**. Do role **RODC** řadiče lze povýšit jakýkoliv počítač, na kterém běží Windows Server 2008 nebo novější. Instalace se provádí stejně jako u normálních řadičů domény. (I Windows **Server 2008 Core** může plnit úlohu **RODC** řadiče, je však potřeba provést bezobslužnou instalaci). Je také možné delegovat instalaci **RODC** řadiče na uživatele, jenž není správce domény. Stačí předpřipravit účet pro instalovaný **RODC** řadič v organizační jednotce Řadiče domény (*Domain Controllers*) a specifikovat učet, jenž bude použit pro připojení tohoto řadiče do domény. Server, který bude povýšen do role **RODC** řadiče, musí být člen pracovní skupiny. Pokud by byl v doméně, nebude se moci navázat na předpřipravený účet.

Fine-Grained zásady hesel a uzamykání účtů [Povinné]

Zásady hesel (*Password Policies*) a zásady uzamykání účtů (*Account Lockout Policies*) se nacházejí pod uzlem nastavení počítače (*Computer Configuration*). Tyto zásady jsou tedy vždy aplikovány pouze na počítače, ne na uživatele. Výjimkou jsou nastavení obsažená v **GPO** objektu Default Domain Policy, která jsou aplikována na veškeré uživatele v dané doméně. Pokud bylo dříve potřeba změnit nastavení těchto zásad pouze pro některé uživatele, nebylo to jednoduše možné. Jedinou možností bylo použití speciálních filtrů pro hesla nebo nasazení více domén s odlišným nastavením Default Domain Policy[3]. Od systému Windows Server 2008 lze tento problém řešit pomocí tzv. *fine-grained* zásad hesel.

***Fine-grained* zásady hesel** (*fine-grained password and lockout policies*, či jen *fine-grained policies*) umožňují definovat zásady hesel a uzamykání účtů pro jednotlivé skupiny nebo uživatele v doméně. Aby bylo možné používat tyto zásady v dané doméně, musí být její funkční úroveň alespoň Windows Server 2008.

Objekty nastavení hesel [Povinné]

Zásady spravované *fine-grained* zásadami hesel jsou totožné se zásadami pod uzly Zásady hesla (*Password Policy*) a Zásady uzamčení účtů (*Account Lockout Policy*) v **GPO** objektech. *Fine-grained* zásady hesel ale nejsou implementovány jako součást zásad skupiny, ani nejsou aplikovány jako **GPO** objekty. Jsou uloženy ve speciálním objektu **Active Directory** označovaném Objekt nastavení hesel (**PSO**, *Password Settings Object*). V doméně může existovat neomezené množství **PSO** objektů. **PSO** objekt může být připojen (*linked*) k jedné či více globálním bezpečnostním skupinám (*global security group*) nebo uživatelům. K jiným typům skupin nelze připojit.

Stejně jako u **GPO** objektů, i u **PSO** objektů může být jeden **PSO** objekt přiřazen k více skupinám či uživatelům. Navíc jeden uživatel může být členem hned několika skupin. Na rozdíl od **GPO** objektů ale **PSO** objekty vždy definují veškeré obsažené zásady, tedy vždy pouze jediný **PSO** objekt určuje výsledná nastavení aplikovaná na daného uživatele. Každý **PSO** objekt obsahuje atribut, který určuje jeho prioritu. Priorita je, stejně jako u **GPO** objektů, nezáporné číslo, kdy menší číslo znamená vyšší prioritu. Pokud je na uživatele aplikováno více **PSO** objektů, projeví se nastavení z toho, jenž má nejvyšší prioritu. Pravidla pro určení výsledné priority jsou následující:

- Pokud je ke skupinám, jejichž členem je daný uživatel, připojeno více **PSO** objektů, vybere se ten s nejvyšší prioritou.
- Pokud je jeden nebo více **PSO** objektů připojeno přímo k danému uživateli, jsou **PSO** objekty připojené ke skupinám ignorovány, nezávisle na jejich prioritě. Ze všech **PSO** objektů připojených k danému uživateli se vybere ten s nejvyšší prioritou.

[3] Existuje ještě možnost přepsat některá nastavení u jednotlivých uživatelských účtů (na záložce nastavení účtu ve vlastnostech uživatele), ovšem většina důležitých nastavení tam chybí a také není únosné nastavovat vše pro každého uživatele zvlášť

- Pokud má více **PSO** objektů stejnou prioritu, vybere **Active Directory** ten, jenž má nejnižší hodnotu **GUID** identifikátoru. Jelikož žádné dva objekty v **Active Directory** nemají stejný **GUID** identifikátor, je zajištěno, že takto musí být vybrán pouze jediný **PSO** objekt. Je pouze na uživateli, aby nastavil priority **PSO** objektů tak, aby k této situaci nemohlo dojít.

Active Directory ukládá u každého uživatele informaci o výsledném **PSO** objektu, jenž bude na tohoto uživatele aplikován. Tato informace je uložena ve formě atributu objektu uživatele.

Je důležité si uvědomit, že **PSO** objekty jsou připojovány pouze ke skupinám a uživatelům. Nelze je připojit k organizačním jednotkám, jak tomu je v případě **GPO** objektů. Jedinou možností jak aplikovat nastavení v **PSO** objektu na uživatele v nějaké organizační jednotce je vytvořit novou skupiny, do které se zařadí všichni uživatelé z dané organizační jednotky. Tyto skupiny se často označují jako tzv. stínové skupiny (*shadow groups*).

Replikace Active Directory

[Povinné]

Jedním z hlavních úkolů **Active Directory**, jakožto řešení **IDA**, je *autentizace* bezpečnostních objektů (*security principals*) jako jsou uživatelé nebo počítače. Pro zajištění bezproblémové *autentizace*, a správného fungování řady dalších služeb **Active Directory**, je samozřejmě důležité mít k dispozici veškerá potřebná data. Tento úkol řeší replikace **Active Directory**. Samotný proces replikace není pouze o přesunu dat, nejprve se musí vyřešit, která data je potřeba přesunout a kudy tento přesun vést.

První problém, která data přesouvat, se řeší pomocí oddílů **Active Directory** databáze. Zde pouze stačí specifikovat, které oddíly se mají replikovat. Druhý problém, kudy data přesouvat, je podstatně náročnější, jelikož jeho řešení se může dynamicky měnit. Výběr cesty (posloupnosti linek) je závislý na topologii sítě a také na charakteristikách a vytížení linek v této síti. Stejně jako **Active Directory** reprezentuje uživatele nebo počítače pomocí odpovídajících typů objektů, tak také topologii reprezentuje pomocí specifických typů objektů.

Místa

[Povinné]

Místo (*site*), v obecném slova smyslu, je fyzické umístění (např. kancelář či město). Tyto místa jsou propojena pomocí spojení (linek). Společně pak místa a spojení vytvářejí topologii (či infrastrukturu) sítě. **Active Directory** reprezentuje infrastrukturu sítě pomocí objektů míst (*site*) a linek (*site link*).

Objekty míst slouží k lokalizaci služeb a ovlivňují celý proces replikace. Jsou umístěny v kontejneru konfigurace (*Configuration*) v kořenové doméně lesa a slouží k:

- **Správě replikačního provozu**[4]. Replikace není nic jiného než přenos změn v **Active Directory** databázi na ostatní řadiče domény. **Active Directory** rozlišuje dva typy sítí v podniku. Prvním typem jsou tzv. *highly connected* sítě, které se vyznačují rychlou konektivitou a vysokou propustností. Replikace v těchto sítích je prováděna okamžitě (jakmile dojde ke změně v **Active Directory** databázi) a je dokončena v rámci sekund. Tento typ sítě reprezentují právě objekty míst. Druhým typem jsou tzv. *less highly connected* sítě, které mívají pomalé či nespolehlivé spojení mezi svými uzly. Replikace v těchto sítích je často plánována a prováděna jen v předem nastavených intervalech. Do tohoto typu sítí lze zařadit sítě mezi jednotlivými místy.
- **Usnadnění lokalizace služeb**. V **Active Directory**, jakožto distribuovaném systému, může některé služby poskytovat více serverů, např. všechny řadiče domény mohou *autentizovat* daného uživatele. Z pohledu klienta je ovšem nejvýhodnější kontaktovat nejbližší[5] server, jenž požadovanou službu poskytuje. Objekty míst, tedy místa z pohledu **Active Directory**, pomáhají při lokalizaci služeb. Klienti vždy mají informaci o tom, ve kterém místě se nacházejí. Jakákoliv distribuovaná služba může tedy využít tyto informace pro lepší lokalizaci svých služeb.

[4] Replikačním provozem (*replication traffic*) je myšlen síťový provoz týkající se pouze replikovaných dat

[5] Nejde o fyzickou vzdálenost, ale o vzdálenost na základě metriky zachycující rychlost konektivity a propustnost

Objekty míst v **Active Directory** nemusí vždy přesně odpovídat místům fyzickým. Někdy může být výhodné zahrnout více fyzických míst do jediného **Active Directory** místa (reprezentovat je jediným objektem míst), např. v situaci, kdy je mezi těmito místy rychlé a spolehlivé spojení. Stejně tak může být dobré rozdělit jedno fyzické místo na více **Active Directory** míst. Toto rozdělení nemá příliš smysl z hlediska replikace, ale lze tak vynutit využívání distribuovaných služeb v rámci menších lokalit v případě, že fyzické místo je již příliš rozsáhlé.

Objekty míst slouží zároveň jako kontejnery pro objekty podsítí (*subnet*). Každý objekt místa může obsahovat více objektů podsítí, ale každý objekt podsítě může být přiřazen pouze jedinému objektu místa. Objekt podsítě definuje rozsah IP adres. Tyto objekty jsou důležité pro lokalizaci služeb. Pokud se počítač připojí do domény, je na základě jeho IP adresy zjištěno, pod který objekt podsítě náleží (neboli do kterého rozsahu IP adres spadá). Protože každý objekt podsítě je jednoznačně přiřazen právě k jednomu místu, lze jednoduše určit, ve kterém místě se počítač nachází.

Speciálním případem určování náležitosti počítačů do míst jsou řadiče domény. První řadič domény v novém lese (*forest*) je automaticky umístěn do objektu místa **Default-First-Site-Name**. Další řadiče domény jsou poté přidávány do míst na základě jejich IP adresy. Toto zařazení lze ovšem kdykoliv změnit a řadič domény přemístit do jiného objektu místa i v případě, že má IP adresu, jenž nespadá pod žádný rozsah objektů podsítí pod tímto cílovým objektem místa. Tedy umístění řadičů domén do jednotlivých míst je nezávislé na jejich IP adrese. Tento způsob také zaručuje jednoznačné přiřazení řadičů domén do míst a to i v případě řadičů domén obsahujících více síťových rozhraní. Tyto řadiče by, na základě svých IP adres, jinak mohly spadat pod více míst zároveň.

Úkoly replikace

[Povinné]

Jak již bylo zmíněno dříve, přesun dat je pouze jedním z úkolů, jenž replikace řeší. Obecně lze říci, že replikace **Active Directory** zajišťuje:

- **Rozdělení úložiště dat**. Databáze **Active Directory** je rozdělena do více oddílů. Některé oddíly jsou přítomny implicitně (ihned po instalaci), další je možné kdykoliv přidat. Cílem tohoto rozdělení je minimalizovat množství replikovaných dat. Vždy se replikují data pouze těch oddílů, které jsou potřeba. Oddíl lze tedy považovat za nejmenší jednotku replikace dat, nikdy nelze nastavit replikaci jen části nějakého oddílu. Například řadiče domény obsahují oddíl domény (*domain naming context*), jenž zahrnuje informace (objekty) o jejich doméně. Tento oddíl je replikován pouze na ty řadiče domény, které leží ve stejné doméně. Globální katalog je zase umístěn v jiném oddíle **Active Directory**. Ten je replikován jen na ty řadiče domény v daném lese, které plní funkci globálního katalogu.
- **Automatické vytváření replikační topologie**. Replikační topologie zachycuje cesty v síti, které budou použity pro přesun dat. Standardně vytváří **Active Directory** dvoucestnou topologii. To znamená, že z jednoho uzlu (řadiče domény) do druhého existují dvě různé cesty. V případě, že dojde k výpadku nějakého uzlu, pořád existuje alternativní cesta pro realizaci přesunu dat. Tato topologie se samozřejmě v průběhu času dynamicky mění, jelikož řadiče domény můžou být přidávány, odebírány nebo přesouvány mezi místy.
- **Replikaci na úrovni atributů**. Výběr dat pro replikaci je sice realizován na úrovni oddílů databáze **Active Directory**, to ovšem neznamená, že musí být přesouvána veškerá tato data. Vždy dochází pouze k přenosu dat popisujících nastalé změny. Jakmile je změněn atribut nějakého objektu, je replikován pouze tento atribut (případně další dodatečné informace blíže popisující danou změnu).
- **Odlišnou místní (*intrasite*) a mezimístní (*intersite*) replikaci**. Replikace v rámci jednoho místa bude probíhat jinak (ihned) než replikace mezi dvěma místy (plánovaně).
- **Detekci a řešení kolizí**. Jelikož změny v **Active Directory** databázi mohou být provedeny kdykoliv a kterýmkoliv řadičem domény, může se stát, že jeden atribut bude změněn zároveň na dvou řadičích domény. V takovémto případě musí replikace zajistit vyřešení tohoto konfliktu.

Replikační topologie

[Povinné]

Hlavní úlohu při vytváření replikační topologie hrají objekty spojení (*connection objects*). Objekty spojení reprezentují spojení mezi dvěma řadiči domény. Toto spojení je vždy jednosměrné a to pouze v příchozím (*inbound*) směru. Spojení také definuje replikační partnery. Pokud existuje objekt spojení definující spojení z prvního řadiče domény do druhého, je první řadič domény replikačním partnerem druhého (opačně to neplatí, jelikož je spojení jednosměrné) [6]. Replikace v **Active Directory** patří mezi tzv. *pull* technologie. Jednotlivé řadiče domény si stahují změny od svých replikačních partnerů.

I pokud neexistuje žádné spojení mezi dvěma řadiči domény (není definován žádný objekt spojení, jenž obsahuje dané dva řadiče domény), je potřeba zaručit, že změny provedené na jednom z nich se projeví také na druhém, tedy že bude provedena replikace. Tento úkol zajišťují replikační cesty. Replikační cesta je posloupnost následných spojení mezi jednotlivými dvojicemi řadičů domény. Definuje tedy, po kterých spojeních (přes které objekty spojení) se lze dostat z jednoho řadiče domény na jiný. Replikační topologie lesa je pak tvořena všemi těmito replikačními cestami.

Vytváření replikační topologie zajišťuje jedna z komponent **Active Directory** označovaná jako **KCC** (*Knowledge Consistency Checker*). **KCC** vytváří dvoucestnou topologii s maximálním počtem tří skoků. Tedy maximální délka replikační cesty (počet průchozích spojení) mezi kterýmikoliv dvěma řadiči domény nesmí být větší než tři. **KCC** automaticky vytváří objekty spojení, aby dosáhlo požadované replikační topologie. Pokud je do místa přidán nebo z místa odebrán nějaký řadič domény, případně když některý řadič domény nereaguje, upraví **KCC** stávající replikační topologii přidáním či odebráním nových objektů, aby opět dosáhl efektivní replikace. Objekty spojení je možné vytvořit i manuálně. Tyto objekty jsou pak perzistentní (nemohou být smazány **KCC** při přetváření replikační topologie).

Místní replikace

[Povinné]

Místní (*intrasite*) replikace se týká replikace změn pouze v rámci jediného místa (*site*). Existují dva odlišné způsoby, jak iniciovat replikaci, buď pomocí oznámení anebo vyzývání.

Oznámení (*notification*) používá zdrojový řadič domény, který provedl změnu v některém ze svých **Active Directory** oddílů. Tento zdrojový řadič může být replikačním partnerem více jiných cílových řadičů domény. Po uplynutí tzv. *initial notification delay* doby (ve výchozím nastavení 15 sekund) zašle zdrojový řadič domény oznámení, že u něj došlo ke změně, jednomu z cílových řadičů domény. Pak vždy po uplynutí tzv. *subsequent notification delay* doby (ve výchozím nastavení 3 sekundy) zašle toto oznámení dalšímu z cílových řadičů domény.

Jakmile cílový řadič domény přijme oznámení o změně, vyžádá si tyto změny od zdrojového řadiče domény. Přenos změn je realizován agentem replikace adresáře (**DRA**, *Directory Replication Agent*), jenž provádí replikaci na úrovni atributů. Po uložení replikovaných změn se z cílového řadiče domény stane zdrojový a celý proces se opakuje tak dlouho, dokud nejsou změny replikovány na všechny potřebné řadiče domény. Protože replikační topologie vytvořená pomocí **KCC** zajišťuje, že do tří skoků se dostanou změny k jakémukoliv řadiči domény, proběhne většinou replikace změn do jedné minuty.

Vyzývání (*polling*) používají cílové řadiče domény. Pokud delší dobu nedostane cílový řadič žádné oznámení od některého ze svých replikačních partnerů, je potřeba zjistit příčinu. Tento stav může být způsoben tím, že u daného replikačního partnera prostě nedošlo k žádným změnám. Ovšem může to být také tím, že je tento replikační partner nedostupný. Cílový řadič domény tedy kontaktuje tohoto replikačního partnera a dotáže se, zda u něj došlo ke změnám. Tento proces se označuje jako vyzývání a ve výchozím nastavení se provádí co jednu hodinu. Pokud replikační partner neodpovídá, spustí cílový řadič domény **KCC**, jenž provede ověření replikační topologie a její úpravu, pokud je vyzývaný replikační

[6] Někdy se označují oba řadiče domény jako replikační partneři, pak se první řadič domény, u kterého je spojení v odchozím směru, označuje jako tzv. *upstream* (odesílající) replikační partner a druhý řadič domény, u kterého je spojení v příchozím směru, jako tzv. *downstream* (přijímající) replikační partner

partner opravdu nedostupný. Pokud odpoví a oznámí, že u něj došlo ke změnám, budou ty-to změny replikovány.

Mezimístní replikace

[Povinné]

V rámci jednoho místa **KCC** předpokládá, že každé dva řadiče domény jsou síťově dostupné, tedy že každý řadič domény může kontaktovat kterýkoliv jiný řadič domény v daném místě. **KCC** v případě míst tedy úplně ignoruje síťovou topologii níže. Mezi místy lze ovšem vyjádřit síťové cesty, po kterých má replikace probíhat, pomocí objektů linek (*site link*). Objekty linek mohou zahrnovat dva nebo více míst a reprezentují jednu z možných replikačních cest. Objekty linek nijak nespecifikují, která síťová cesta bude při replikaci použita, pouze říkají, že mezi jakýmikoliv dvěma místy v daném objektu linky lze replikaci provést. Tedy že mezi každými dvěma místy v daném objektu linky existuje alespoň jedna síťová cesta, kterou je možné použít pro replikaci. Na rozdíl od objektu spojení, objekty linek musí být vždy vytvářeny manuálně.

Vytváření mezimístní replikační topologie zajišťuje generátor mezimístní topologie (**ISTG**, *Intersite Topology Generator*), jedna z komponent **KCC**. **ISTG** vytváří objekty spojení na základě definovaných objektů linek. Tyto objekty spojení pak určují konkrétní replikační cesty. Efektivita vytvořené replikační topologie je silně závislá na definovaných objektech linek. Není vhodné do jednoho objektu linek umístit dvě místa, jež nejsou přímo fyzicky propojena. Objekty linek by vždy měly odrážet strukturu síťové topologie níže.

Pro replikaci změn mezi místy lze využít dva protokoly:

- **DS-RPC** (*Directory Service Remote Procedure Call*). Tento protokol je výchozí a upřednostňovaný protokol pro mezimístní replikaci. Jako jediný může replikovat oddíl domény.
- **ISM-SMTP** (*Inter-Site Messaging Simple Mail Transport Protocol*). Tento protokol se používá, pokud je spojení mezi místy nespolehlivé nebo ne vždy k dispozici. Velkou nevýhodou tohoto protokolu je, že vyžaduje pro svou funkcionalitu přítomnost certifikační autority (CA) a také, že nemůže replikovat oddíl domény.

Bridgehead servery

[Povinné]

ISTG vytváří replikační topologii mezi místy obsaženými v nějakém objektu linky. Aby byla replikace realizována maximálně efektivně, je v každém místě vybrán jeden řadič domény, který bude plnit úlohu tzv. *bridgehead* serveru. *Bridgehead* servery mají na starosti replikaci zvoleného oddílu **Active Directory** mezi jednotlivými místy. Pokud dojde ke změně v nějakém oddílu **Active Directory**, proběhne v místě, kde k této změně došlo, místní replikace. Změna bude tedy replikována na ostatní řadiče domény v daném místě. Jakmile informace o této změně dorazí k řadiči domény, jenž je *bridgehead* server pro daný oddíl, replikuje tento řadič domény nastalé změny *bridgehead* serverům v ostatních místech. V těchto místech pak proběhne opět místní replikace. Tento postup zaručuje minimální přenosy dat mezi jednotlivými místy. Změny vždy putují pouze jednou mezi každou dvojicí míst v daném objektu linky.

Bridgehead servery jsou vybírány automaticky, v každém místě vždy jeden pro každý oddíl **Active Directory**. Je tedy možné, aby v jednom místě existovalo i více *bridgehead* serverů, každý pro jiný oddíl **Active Directory**. Pokud ovšem nejsou v daném místě řadiče domény z různých domén a neexistují žádné, uživatelem definované, oddíly aplikací (které by mohly být replikovány pouze na určité řadiče domény a žádný řadič domény by neobsahoval všechny), bývá *bridgehead* server pouze jeden. Pokud dojde k výpadku *bridgehead* serveru, je tato úloha automaticky přesunuta na jiný řadič domény. Lze také explicitně definovat jeden či více řadičů domény, jenž budou upřednostňovány jako *bridgehead* servery. V tomto případě ale platí, že v případě výpadku všech takto specifikovaných řadičů domény již nebude vybrán žádný další a replikace mezi místy selže.

[Povinné]

Další možnosti konfigurace mezimístní replikace

Ne vždy musí být replikační topologie vytvořená **ISTG** ideální. U složitějších sítí může být potřeba přesněji nastavit jednotlivé objekty linek nebo celý proces replikace. Hlavní nastavení se týkají:

- **Tranzitivity objektů linek**. Pokud jeden objekt linky obsahuje místa A a B a druhý objekt zase místa B a C, pak **ISTG** ví, že lze provést replikaci mezi místy A a B a také B a C. V případě, že je zaplá tranzitivita objektů linek, bude to pro **ISTG** znamenat, že může provést replikaci i mezi místy A a C (mohl by být teoreticky vytvořen objekt spojení pro místa A a C). Tranzitivita je ve výchozím nastavení povolena.
- **Mostů objektů linek**. Mosty objektů linek (*site link bridges*) jsou spojení dvou a více objektů linek, jenž vytváří jednu tranzitivní linku. Mosty mají smysl pouze v případě, že je zakázána tranzitivita objektů linek. Pokud je povolena, jsou vytvořené mosty ignorovány.
- **Ceny objektů linek**. Často může být replikace mezi dvěma řadiči domény realizována přes více možných cest. Přiřazením různých cen k jednotlivým objektům linek lze ovlivňovat výběr nejvhodnější cesty ze všech možných. Čím nižší cenu má daný objekt linky, tím více bude tato cesta preferována před ostatními.
- **Frekvence replikace**. Mezimístní replikace je založena výhradně na vyzývání, žádná oznámení nejsou zasílána. Ve výchozím nastavení se každé tři hodiny *bridgehead* server dotazuje svých replikačních partnerů (*bridgehead* serverů z ostatních míst, jenž mají na starosti stejný oddíl **Active Directory**), zda u nich nedošlo k nějakým změnám. Tento interval lze kdykoliv změnit, musí být ovšem alespoň 15 minut.
- **Plánování replikace**. Ve výchozím nastavení probíhá replikace 24 hodin denně. Tyto doby lze omezit jen na určité hodiny, během kterých bude dané spojení (*site link*) mezi místy k dispozici.

Lektorské úkoly

Lab L00 – konfigurace virtuálních stanic

[Provést]

Připojte sítové adaptéry stanic k následujícím virtuálním přepínačům:

Adaptér (MAC suffix)	LAN1 (-01)	LAN2 (-02)	LAN3 (-03)	LAN4 (-04)
w2016-dc	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno
w2016-repl	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno
w2016-base	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno

- v případech, kdy je potřeba přistupovat na externí síť, připojte adaptér **LAN1** k přepínači *Internal*.
- Pro přístup na server **yetti** přes *Internal* síťové rozhraní je nutné použít jeho plně kvalifikované doménové jméno **yetti.nepal.aps**
- Servery D+R+C w2016-dc a D+R+C w2016-repl je nutné spouštět společně

Lab L01 – Instalace RODC

[Provést]

Cíl cvičení

Přidat RODC řadič do existující domény

Potřebné virtuální stroje

w2016-dc (D+R+C w2016-dc)
w2016-repl (D+R+C w2016-repl)
w2016-base

Další prerekvizity

Globální bezpečnostní skupina (*global security group*) **Simpsons** v doméně **testing.local**, účet uživatele **student** v doméně **testing.local**, který není členem skupiny **Simpsons**, účet uživatele **homer** v doméně **testing.local**, jenž je členem skupiny **Simpsons**

1. Na **w2016-base** nastavte statickou IPv4 adresu **192.168.32.7** jako IPv4 adresu počítače a IPv4 adresu **192.168.32.5** jako IPv4 adresu DNS serveru
   a. Otevřete **Network and Sharing Center**, zvolte LAN2 a pak Properties
      - Zvolené síťové rozhraní musí odpovídat *Private1*, standardně to je LAN2
   b. Vyberte Internet Protocol Version 4 (TCP/IPv4) a zvolte Properties
   c. Zvolte Use the following IP address a jako IP address zadejte **192.168.32.7**
   d. Klikněte do zadávacího pole u Subnet mask, maska podsítě bude doplněna automaticky
   e. Pod Use the following DNS server addresses zadejte **192.168.32.5** do pole Preferred DNS Server
   f. Potvrďte OK a dvakrát Close
2. Nainstalujte roli **Active Directory Domain Services**
   a. Spusťte **Server Manager**
      1. Start → **Server Manager**
   b. Vyberte Add Roles and Features z nabídky Manage
   c. Pokračujte Next >
   d. Vyberte Role-based or feature-based installation a pokračujte Next >

e. Vyberte aktuální server a pokračujte Next >
f. V seznamu rolí vyberte Active Directory Domain Services, potvrďte přidání potřebných funkcí Add Features a pokračujte třikrát Next >
g. Potvrďte instalaci Install
h. Po dokončení instalace najdete v notifikacích Server Manageru odkaz na Promote this server to a domain controller

3. V konfiguračním průvodci (Active Directory Domain Services Configuration Wizard)
   a. V kroku Deployment Configuration
      1. Zvolte Add a domain to an existing forest
      2. Do pole Domain zadejte **testing.local**
      3. Klepněte na tlačítko Change… v sekci Supply the credentials to perform this operation a vyplňte jméno **testing\administrator** a heslo **aaa**
      ➢ Lze použít i zápis **administrator@testing.local**
      4. Pokračujte Next >
   b. V části Domain Controller Options
      1. ponechte zaškrtnuté možnosti **DNS server** i **Global Catalog**
      2. zaškrtněte **Read-only Domain Controller (RODC)**.
      3. v Site name ponechte místo **Default-First-Site-Name**
      4. Jako Directory Services Restore Mode (DSRM) Password použijte (a potvrďte) heslo **aaa**
      5. pokračujte Next >
   c. V části RODC Options zvolte skupinu **Simpsons** jako správce instalovaného RODC řadiče
      1. Pod Delegated administrator account použijte Select…
         a. V Enter the object names to select zadejte **Simpsons** a zvolte Check Names pro ověření existence zadané skupiny
         b. Potvrďte OK
      2. Zkontrolujte uživatelské skupiny, jejichž hesla se budou/nebudou replikovat na tento RODC
      3. Pokračujte Next >
   d. V části Additional Options zvolte, odkud proběhne úvodní replikace
      1. Z nabídky Replicate from zvolte **w2016-dc.testing.local**
      2. Pokračujte Next >
   e. Zadejte cesty k databázím Location for Database, Log Files, and SYSVOL (ponechte výchozí). Next >
   f. Zkontrolujte zadané údaje a zobrazte si odpovídající **skript pro PowerShell** (View Script). Pokračujte Next >
   g. Prohlédněte si výsledky kontroly prerekvizit.
4. Přihlaste se na **w2016-base** jako uživatel **student**
   ➢ Přihlášení nebude úspěšné, jelikož standardní uživatel nemá právo přihlašovat se lokálně na řadiče domény (nepatří mezi lokální administrátory)
5. Přihlaste se na **w2016-base** jako uživatel **homer**
   ➢ Přihlášení bude úspěšné, jelikož skupina **Simpsons** patří mezi lokální administrátory, kteří jsou na rozdíl od normálních řadičů domény přítomni, u normálních řadičů domény patří mezi lokální administrátory vždy pouze členové **Domain Admins** skupiny bez možnosti to jakkoliv změnit

Lab L02 – ADSS (Active Directory Sites and Services) [Na cvičeních]

Lab L03 – Vytvoření replikační topologie [Provést]

Cíl cvičení

Manuálně vytvořit vlastní replikační topologii pomocí míst a spojení

Potřebné virtuální stroje

w2016-dc (D+R+C w2016-dc)
w2016-repl (D+R+C w2016-repl)
w2016-base

Další prerekvizity

Dokončený úkol **L01**, objekt linky (*site link object*) **BRNO** v kontejneru IP z úkolu **L02**

1. Na **w2016-dc** otevřete **ADSS** (*Active Directory Sites and Services*)
   a. Start → Administrative Tools → **Active Directory Sites and Services**
2. Vytvořte nové místo s názvem **VUT**
   a. Klikněte pravým na kontejner Sites a zvolte New Site…
   b. Jako název (Name) zadejte **VUT** a pod Select a site link object for this site vyberte objekt linky **BRNO**
   c. Potvrďte vytvoření místa dvakrát pomocí OK
3. Vypněte automatické generování místní a mezimístní replikační topologie pro místo **VUT**
   a. Vyberte místo **VUT**
   b. V okně napravo klikněte pravým na NTDS Site Settings a zvolte Properties
   c. Přejděte na záložku Attribute Editor, vyberte atribut **options** a zvolte Edit
   d. Zadejte hodnotu (Value) **0x11** a potvrďte dvakrát OK
      - Nastavení 1. nejnižšího bitu (hodnota **0x01**) vypíná generování místní replikační topologie, nastavení 5. nejnižšího bitu (hodnota **0x10**) zase vypíná generování mezimístní replikační topologie
4. Přesuňte **w2016-dc** do místa **VUT**
   a. Klikněte pravým na server **w2016-dc** a zvolte Move…
   b. Pod Select the site that should contain this server zvolte místo **VUT**
   c. Potvrďte přesun pomocí OK
5. Přesuňte **w2016-repl** do místa **VUT** podle postupu z **bodu 4**
6. Vytvořte místo **FIT**, vypněte v něm automatické generování místní a mezimístní replikační topologie a přesuňte do něj server **w2016-base** podle postupů z **bodů 2 - 4**
7. Smažte všechny objekty spojení zahrnující **w2016-dc**, **w2016-repl** a **w2016-base** s výjimkou objektu spojení **RODC Connection (SYSVOL)** u **w2016-base**
   a. Klikněte pravým na konkrétní objekt spojení a zvolte Delete
   b. Potvrďte smazání pomocí Yes
8. Vytvořte spojení z **w2016-dc** do **w2016-repl** a názvem **dc2repl**
   a. Klikněte pravým na uzel NTDS Settings pod uzlem **w2016-repl** a vyberte New Active Directory Domain Services Connection…
   b. Ze Search result vyberte **w2016-dc** a zvolte OK
   c. Jako název (Name) zadejte **dc2repl** a vytvořte objekt spojení pomocí OK
9. Upravte spojení **RODC Connection (SYSVOL)** tak, aby byl replikačním partnerem **w2016-base** **w2016-dc**, tedy aby **w2016-base** replikoval změny vždy od **w2016-dc**

a. Klikněte pravým na objekt spojení **RODC Connection (SYSVOL)** a zvolte Properties
b. Na záložce General v části Replicate from zvolte Change...
c. Ze Search result vyberte **w2016-dc** a potvrďte dvakrát OK

10. Zavřete a znova otevřete **ADSS** (*Active Directory Sites and Services*)
    - Konzole může po dříve provedených úpravách stále obsahovat staré objekty, které nejsou odstraněny ani v případě aktualizace (refresh) konzole, při uzavření konzole jsou ale tyto objekty vždy odstraněny a při následném otevření již konzole obsahuje aktuální objekty
11. Replikujte změny v konfiguraci **Active Directory** na ostatní řadiče domény
    a. Klikněte pravým na uzel NTDS Settings pod uzlem **w2016-repl** resp. **w2016-base** a zvolte Replicate configuration to the selected DC
       - Pokud replikace selže, přejděte (připojte se pomocí **ADSS**) na **w2016-repl** resp. **w2016-base**, klikněte pravým na uzel NTDS Settings pod uzlem **w2016-dc** a zvolte Replicate configuration from the selected DC
12. Promítněte změny do replikační topologie **Active Directory**
    a. Na všech řadičích domény spusťte jako administrátor příkaz **repadmin /kcc**
13. Na **w2016-dc** proveďte nějakou změnu v **Active Directory** databázi, například u uživatele **homer** změňte hodnotu atributu Description
14. Zjistěte, na které řadiče domény byla změna replikována
    a. Ověřte, že na **w2016-repl** byla změna replikována
       - Změny se projeví až za cca. 15 sekund, až po 15 sekundách bude totiž zasláno oznámení prvnímu z řadičů domény v daném místě, jehož replikačním partnerem je **w2016-dc**, v tomto případě tedy řadiči domény **w2016-repl**
    b. Ověřte, že **na w2016-base** nedošlo k žádným změnám
       - **Pozor** na používání **ADUC** konzole na **RODC** řadičích, tato konzole se primárně připojuje k normálním řadičům domény, které mohou zapisovat do **Active Directory** databáze, po otevření této konzole může být potřeba změnit řadič domény (kliknout pravým na Active Directory Users and Computers a vybrat Change Domain Controller…), jinak pak konzole zobrazuje stav **Active Directory** databáze na jiném řadiči domény
       - Změny se projeví do 3 hodin, což je výchozí interval pro vyzývání, jenž je jediná možnost jak iniciovat mezimístní replikaci
15. Vynuťte replikaci změn provedených na **w2016-dc** na **w2016-base**
    a. Vyberte uzel NTDS Settings pod uzlem **w2016-base**
    b. Klikněte pravým na spojení **RODC Connection (SYSVOL)** a zvolte Replicate Now
    c. Potvrďte OK
16. Ověřte, že změna byla replikována na **w2016-base**
17. Proveďte nějakou změnu v **Active Directory** databázi tentokrát na **w2016-repl**
18. Ověřte, že změna nebyla replikována na žádný z ostatních řadičů domény
    - Spojení jsou vždy jednosměrná, vytvořené spojení **dc2repl** umožňuje replikovat změny pouze z **w2016-dc** na **w2016-repl**, nikdy ne opačně
19. Vytvořte spojení z **w2016-repl** zpět na **w2016-dc** s názvem **repl2dc** podle postupu z **bodu 8**
20. Replikujte změny v konfiguraci na ostatní řadiče domény a promítněte je do replikační topologie podle postupů z **bodů 11 - 12**
21. Ověřte, že změny byly replikovány na **w2016-dc**

Studentské úkoly

- Na všech stanicích zakažte *Internal* síťové rozhraní (**LAN1**) a povolte ho pouze v případech, že je potřeba přistupovat na externí síť!!!

Lab S01 – Bridgehead servery a mezimístní replikační topologie [Povinné]

Cíl cvičení

Nastavit upřednostňované bridgehead servery, automaticky vygenerovat replikační topologii a ověřit její správnost

Potřebné virtuální stroje

w2016-dc (D+R+C w2016-dc)
w2016-repl (D+R+C w2016-repl)
w2016-base

Další prerekvizity

Dokončený úkol **Lab L01**, místo **VUT** obsahující servery **w2016-dc** a **w2016-repl**, místo **FIT** obsahující server **w2016-base**, objekt linky (*site link object*) obsahující oba místa **VUT** a **FIT**

1. Na **w2016-dc** otevřete **ADSS** (*Active Directory Sites and Services*)
   a. Start → Administrative Tools → **Active Directory Sites and Services**
2. Smažte všechny objekty spojení zahrnující **w2016-dc**, **w2016-repl** a **w2016-base**
   a. Klikněte pravým na objekt spojení a zvolte Delete
   b. Potvrďte smazání pomocí Yes
      - Pokud objekt spojení nepůjde smazat, ověřte, že není chráněn proti smazání
        1. Klikněte pravým na objekt spojení a zvolte Properties
        2. Přejděte na záložku Object
        3. Odškrtněte možnost Protect object from accidental deletion
        4. Potvrďte pomocí OK
3. Nastavte **w2016-dc** jako **ISTG** (*Intersite Topology Generator*) pro místo **VUT**
   a. Vyberte místo **VUT**
   b. V okně napravo klikněte pravým na NTDS Site Settings a zvolte Properties
   c. Přejděte na záložku Attribute Editor, vyberte atribut **interSiteTopologyGenerator** a zvolte Edit
   d. Zadejte hodnotu **CN=NTDS Settings,CN=W2016-DC,CN=Servers,CN=VUT,CN=Sites, CN=Configuration,DC=testing,DC=local**
4. Povolte automatické generování místní a mezimístní replikační topologie pro místo **VUT**
   a. Vyberte místo **VUT**
   b. Klikněte pravým na NTDS Site Settings v okně napravo a zvolte Properties
   c. Přejděte na záložku Attribute Editor, vyberte atribut **options** a zvolte Edit
   d. Zvolte Clear a potvrďte pomocí OK
5. Nastavte **w2016-dc** jako **ISTG** pro místo **FIT** a povolte pro toto místo generování místní a mezimístní replikační topologie podle postupu z **bodů 3 – 4**
6. Nastavte **w2016-dc** jako upřednostňovaný bridgehead server pro místo **VUT**
   a. Klikněte pravým na uzel **w2016-dc** a zvolte Properties
   b. Pod Transports available for inter-site data transfer vyberte **IP** a zvolte Add >>
   c. Potvrďte pomocí OK

7. Vygenerujte místní replikační topologii pro místo **VUT**
   a. Klikněte pravým na NTDS Settings pod uzlem **w2016-dc** a pod All Tasks zvolte Check Replication Topology
   b. Potvrďte pomocí OK
   c. Opakujte **body a – b** pro uzel **w2016-repl**
8. Ověřte automatické vytvoření spojení mezi **w2016-dc** a **w2016-repl**
   a. Pokud nejsou objekty spojení pod NTDS Settings viditelné, klikněte pravým na uzel NTDS Settings a zvolte Refresh
9. Vygenerujte mezimístní replikační topologii mezi místy **FIT** a **VUT**
   a. Klikněte pravým na uzel NTDS Settings pod uzlem **w2016-base** a pod All Tasks zvolte Check Replication Topology
   b. Potvrďte pomocí OK
10. Na **w2016-base** ověřte, že bylo vytvořeno spojení z **w2016-dc** do **w2016-base**
    a. Na **w2016-base** otevřete **ADSS** (*Active Directory Sites and Services*)
       1. Start → Administrative Tools → **Active Directory Sites and Services**
    b. Připojte se k **w2016-base**
       1. Klikněte pravým na Active Directory Users and Computers a zvolte Change Domain Controller…
       2. Pod Change to zvolte možnost This Domain Controller or AD LDS instance a vyberte **w2016-base.testing.local**
       3. Potvrďte dvakrát pomocí OK
    c. Vyberte uzel NTDS Settings pod uzlem **w2016-base**
    d. Zkontrolujte, že vygenerované spojení (objekt spojení) jde z (From Server) **w2016-dc**
11. Vraťte se zpátky na **w2016-dc** a zrušte **w2016-dc** jako upřednostňovaný bridgehead server pro místo **VUT**
    a. Klikněte pravým na uzel **w2016-dc** a zvolte Properties
    b. Pod This server is a preferred bridgehead server for the following transports vyberte IP a zvolte << Remove
    c. Potvrďte pomocí OK
12. Nastavte **w2016-repl** jako upřednostňovaný bridgehead server pro místo **VUT** podle postupu z **bodu 6.a**
13. Přegenerujte mezimístní replikační topologii mezi místy **FIT** a **VUT** podle postupu z **bodu 9**
14. Na **w2016-base** ověřte, že bylo vytvořeno spojení z **w2016-repl** do **w2016-base**
    - Pokud spojení nebylo vytvořeno, proveďte postup z **bodu 9** na **w2016-base**

Lab S02 – Zásady replikace hesel [Volitelné]

Cíl cvičení

Umožnit ukládání hesel vybraných uživatelů ve vyrovnávací paměti RODC řadiče

Potřebné virtuální stroje

w2016-dc (D+R+C w2016-dc)
w2016-repl (D+R+C w2016-repl)
w2016-base

Další prerekvizity

Dokončený úkol **Lab L01**, účty uživatelů **homer** a **bart** v doméně **testing.local**, kteří jsou členy skupiny **Simpsons**

1. Na **w2016-dc** otevřete **ADUC** (*Active Directory Users and Computers*)
   a. Start → Administrative Tools → **Active Directory Users and Computers**
2. Povolte pro všechny uživatele ze skupiny **Simpsons** ukládání hesel do vyrovnávací paměti na **w2016-base**
   a. Vyberte organizační jednotku Domain Controllers, klikněte pravým na **w2016-base** a zvolte Properties
   b. Přejděte na záložku Password Replication Policy a zvolte Add…
   c. Vyberte Allow passwords for the account to replicate to this RODC a pokračujte pomocí OK
   d. Do Enter the object names to select zadejte **Simpsons** a zvolte Check Names
   e. Potvrďte dvakrát pomocí OK
3. Přihlaste se na **w2016-base** jako uživatel **homer**
4. Ověřte, že heslo bylo skutečně uloženo ve vyrovnávací paměti **w2016-base**
   a. Vyberte organizační jednotku Domain Controllers, klikněte pravým na **w2016-base** a zvolte Properties
   b. Přejděte na záložku Password Replication Policy a zvolte Advanced…
   c. Na záložce Policy Usage zvolte Accounts whose passwords are stored on this Read-only Domain Controller pod Display users and computers that meet the following criteria
   d. Ověřte, že uživatel **homer** je v seznamu pod Users and computers
5. Vložte heslo uživatele **bart** do vyrovnávací paměti **w2016-base**
   a. Vyberte organizační jednotku Domain Controllers, klikněte pravým na **w2016-base** a zvolte Properties
   b. Přejděte na záložku Password Replication Policy a zvolte Advanced…
   c. Na záložce Policy Usage zvolte Prepopulate Passwords…
   d. Do Enter the object names to select zadejte **bart** a zvolte Check Names
   e. Potvrďte pomocí OK, Yes a OK
6. Přerušte spojení mezi w2016-base a ostatními řadiči domény
   a. Na **w2016-dc** a **w2016-repl** zakažte síťové rozhraní LAN2
      ➢ Zakázané síťové rozhraní musí odpovídat *Private1*, standardně to je LAN2
7. Zkuste se přihlásit na **w2016-base** jako uživatel **administrator**
      ➢ Přihlášení nebude úspěšné, protože heslo uživatele **administrator** není obsaženo ve vyrovnávací paměti **w2016-base**
8. Zkuste se přihlásit na **w2016-base** jako uživatel **bart**

- Přihlášení bude úspěšné, jelikož heslo uživatele **bart** bylo přidáno do vyrovnávací paměti **w2016-base**

Lab S03 – Fine-Grained zásady hesel s použitím ADAC

[Volitelné]

Cíl cvičení

Nastavit různé zásady hesel pro jednotlivé uživatele (skupiny) s pomocí Active Directory Administrative Center

Potřebné virtuální stroje

w2016-dc (D+R+C w2016-dc)
w2016-repl (D+R+C w2016-repl)

Další prerekvizity

Účet uživatele **homer** v doméně **testing.local**, který jsou členy skupiny **Simpsons**

1. Na **w2016-dc** otevřete **ADAC** (*Active Directory Administrative Center*)
   a. Start → Administrative Tools → **Active Directory Administrative Center**
2. Přejděte do testing (local) \ System \ Password Settings Container
3. Klikněte pravým a zvolte New \ Password Settings
   a. Nastavte
      1. Name: **Simpsons PSO**
      2. Precedence: **1**
      3. Enforce minimum password length: **3**
      4. Zrušte zaškrtnutí Enforce password history
      5. Ponechte Password must meet complexity requirements
      6. Zrušte zaškrtnutí Enforce minimum password age
      7. Enforce maximum password age: **90**
      8. Zaškrtněte Enforce account lockout policy
      9. Account will be locked out – For a duration of (mins): **1440**
      10. Number of failed logon attempt allowed: **5**
      11. Reset failed logon attempts count after: **60**
   b. V sekci Directly Applies To přidejte skupinu **Simpsons**
      1. Add…
      2. Do Enter the object names to select zadejte **Simpsons** a zvolte Check Names
      3. Potvrďte pomocí OK
   c. Pokračujte OK
4. Zjistěte, jaké zásady hesel se vztahují na uživatele **homer**
   a. Přejděte do testing (local) \ Users
   b. Klikněte pravým na uživatele **homer** vyberte View resultant password settings…
5. Zkuste nastavit uživateli **homer** nové heslo **bbb**
   a. Přejděte do testing (local) \ Users
   b. Klikněte pravým na uživatele **homer** vyberte Reset password…
   c. Zadejte heslo **bbb**
      - Heslo nepůjde vytvořit, jelikož **Simpsons PSO** vyžaduje silná hesla

Lab S04 – Fine-Grained zásady hesel s pomocí ADSI Edit [Volitelné]

Cíl cvičení

Nastavit různé zásady hesel pro jednotlivé uživatele s využitím nástroje ADSI Edit (používáno před příchodem Windows 2012)

Potřebné virtuální stroje

w2016-dc (D+R+C w2016-dc)
w2016-repl (D+R+C w2016-repl)

Další prerekvizity

Účet uživatele **homer** v doméně **testing.local**, který jsou členy skupiny **Simpsons**

1. Na **w2016-dc** otevřete **ADSI Edit** (*Active Directory Services Interfaces Editor*)
   a. Start → Administrative Tools → **ADSI Edit**
2. Připojte se k oddílu domény **testing.local**
   a. Klikněte pravým na ADSI Edit a zvolte Connect to…
   b. Do pole Name zadejte **testing.local** a potvrďte pomocí OK
3. Vytvořte nový PSO (*Password Settings Object*) objekt **Simpsons PSO**
   a. Vybírejte postupně uzly testing.local, DC=testing, DC=local, CN=System a CN=Password Settings Container
   b. Klikněte pravým na uzel CN=Password Settings Container, vyberte New a zvolte Object…
   c. Pod Select a class zvolte třídu **msDS-PasswordSettings** a pokračujte Next >
   d. U atributu **cn** zadejte do pole Value název **Simpsons PSO** a pokračujte Next >
      - Atribut **cn** obsahuje název PSO objektu
   e. U atributu **msDS-PasswordSetingsPrecedence** zadejte do pole Value hodnotu **1** a pokračujte Next >
      - Atribut **msDS-PasswordSetingsPrecedence** je obdoba *link order* u GPO, jenž udává prioritu PSO objektu, pokud je více PSO objektů přiřazeno jedné skupině či uživateli
   f. U atributu **msDS-PasswordReversibleEncryptionEnabled** zadejte do pole Value hodnotu **False** a pokračujte Next >
      - Atribut **msDS-PasswordReversibleEncryptionEnabled** určuje, zda mají být hesla ukládána pomocí reverzibilního šifrování
   g. U atributu **msDS-PasswordHistoryLength** zadejte do pole Value hodnotu **0** a pokračujte Next >
      - Atribut **msDS-PasswordHistoryLength** udává, kolik naposledy zadaných hesel nesmí uživatel použít při změně hesla
   h. U atributu **msDS-PasswordComplexityEnabled** zadejte do pole Value hodnotu **True** a pokračujte Next >
      - Atribut **msDS-PasswordComplexityEnabled** určuje, zda jsou vyžadována silná hesla
   i. U atributu **msDS-MinimumPasswordLength** zadejte do pole Value hodnotu **3** a pokračujte Next >
      - Atribut **msDS-MinimumPasswordLength** určuje minimální délku hesel
   j. U atributu **msDS-MinimumPasswordAge** zadejte do pole Value hodnotu **0:00:00:00** a pokračujte Next >
      - Atribut **msDS-MinimumPasswordAge** určuje, za jakou dobu je možné nejdříve změnit heslo ve formátu *<dny>:<hodiny>:<minuty>:<sekundy>*

k. U atributu **msDS-MaximumPasswordAge** zadejte do pole Value hodnotu **90:00:00:00** a pokračujte Next >
   - Atribut **msDS-MaximumPasswordAge** určuje, za jakou dobu vyprší platnost hesla ve formátu *<dny>:<hodiny>:<minuty>:<sekundy>*

l. U atributu **msDS-LockoutThreshold** zadejte do pole Value hodnotu **5** a pokračujte Next >
   - Atribut **msDS-LockoutThreshold** udává, po jakém počtu špatně zadaných hesel doj-de k zablokování účtu

m. U atributu **msDS-LockoutObservationWindow** vložte do pole Value hodnotu **0:01:00:00** a pokračujte Next >
   - Atribut **msDS-LockoutObservationWindow** udává, kdy dojde k vynulování počítadla špatně zadaných hesel ve formátu *<dny>:<hodiny>:<minuty>:<sekundy>*

n. U atributu **msDS-LockoutDuration** vložte do pole Value hodnotu **1:00:00:00** a pokračujte Next >
   - Atribut **msDS-LockoutDuration** udává délku zablokování účtu, pokud bylo několikrát zadáno špatné heslo, ve formátu *<dny>:<hodiny>:<minuty>:<sekundy>*

o. Potvrďte vytvoření PSO objektu pomocí Finish
   - V případě výskytu chyby Operation failed. error code: 0x20e7, The modification was not permitted for security reasons. ověřte správně zadané hodnoty výše, tato chyba nastává v případě nemožnosti zpracovat zadané hodnoty **ADSI Edit** konzolí

4. Aplikujte PSO objekt **Simpsons PSO** na uživatele ze skupiny **Simpsons**
   a. Klikněte pravým na objekt CN=Simpsons PSO a zvolte Properties
   b. Na záložce Attribute Editor vyberte atribut **msDS-PSOAppliesTo** a zvolte Edit
   c. Zvolte Add Windows Account…
   d. Do Enter the object names to select zadejte **Simpsons** a zvolte Check Names
   e. Potvrďte třikrát pomocí OK
5. Zjistěte, který PSO objekt má být aplikován na uživatele homer
   a. Otevřete **ADUC** (*Active Directory Users and Computers*)
      1. Start → Administrative Tools → **Active Directory Users and Computers**
   b. Zapněte zobrazení pokročilých vlastností uživatelských účtů
      1. V menu konzole vyberte View a zvolte Advanced Features
   c. Klikněte pravým na uživatele **homer** a zvolte Properties
   d. Přejděte na záložku Attribute Editor
   e. Zvolte Filter níže a vyberte Constructed pod Show read-only attributes
   f. Vyhledejte v seznamu atribut **msDS-ResultantPSO** a ověřte, že obsahuje **CN=Simpsons PSO,CN=Password Settings Container,CN=System,DC=testing,DC=local**
6. Zkuste nastavit uživateli **homer** nové heslo **bbb**
   a. Klikněte pravým na uživatele **homer** a zvolte Reset Password…
   b. Zadejte heslo **bbb**
      - Heslo nepůjde vytvořit, jelikož **Simpsons PSO** vyžaduje silná hesla