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**[1]. 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[2] 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.

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.

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

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

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) [3]. Replikace v **Active Directory** patří mezi tzv. *pull* technologie. Jednotlivé řadiče domény si stahují změny od svých replikačních partnerů.

[3] 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

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 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.

Další možnosti konfigurace mezimístní replikace

[Povinné]

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.

Společné úkoly

- Pro přístup na server **file** (a jiné) přes síťové rozhraní *Default switch* je nutné použít jeho plně kvalifikované doménové jméno **file.nepal.local**
- Přístupové údaje na server **file**: **nepal\hstudent** heslo: **aaa**
- Rozsah IP adres přidělených z *Default switch* se může od níže uvedeného rozsahu lišit.

Lab LS00 – konfigurace virtuálních stanic

[Provést]

Připojte sítové adaptéry stanic k následujícím virtuálním přepínačům:

Adaptér (MAC suffix)	LAN1 (-01)	LAN2 (-02)	LAN3 (-03)	LAN4 (-04)
D+R+C w2016-dc	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno
D+R+C 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 *Default switch*.
- Servery **D+R+C w2016-dc a D+R+C w2016-repl** je nutné spouštět společně.
- Tip: stanice **D+R+C w2016-dc** a **D+R+C w2016-repl** spusťte na začátku cvičení.

Studentské úkoly

Lab X01 – instalace RODC pomocí skriptu

[Provést]

Cíl cvičení

Připravit read-only domain controller pro další úkoly

Potřebné virtuální stroje

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

Další prerekvizity

Složka utils se skripty run_rep.bat a prepare.ps1

1. Na **w2016-base** se přihlaste jako lokální uživatel **administrator**
2. Na **w2016-base** zkopírujte složku utils se skripty
   - ✓ Nejrychleji přetažením do okna rozšířené relace připojení k VM
3. Spusťte skript run_prep.bat
   - ✓ Vyžaduje prepare.ps1
   - ➢ Skript běží cca 7 min a na závěr dojde k restartu VM

Lab X02 – ADSS (Active Directory Sites and Services)

[Projít]

Cíl cvičení

Seznámení s ADSS konzolí

Potřebné virtuální stroje

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

1. Na **w2016-dc** se přihlaste jako uživatel **administrator** do domény **testing.local**
2. Otevřete **ADSS** (*Active Directory Sites and Services*)
   a. Start → Administrative Tools → **Active Directory Sites and Services**
3. Prozkoumejte konzoli ADSS
4. Otevřete kontejneru Subnets
   - ➢ Zde naleznete objekty podsítí – zopakujte si, k čemu slouží.
   - ➢ Z pohledu řadičů jsou objekty podsítí irelevantní, řadiče se do míst umisťují explicitně (viz kontejner Servers pod každým místem)
5. Vytvořte objekt podsítě **192.168.32.0/24**
   a. Klikněte pravým na kontejner Subnets a zvolte New subnet…
   b. Jako Prefix zadejte **192.168.32.0/24**
   c. Objekt podsítě přiřaďte místu **Default-First-Site-Name** jeho vybráním pod Select a site object for this prefix
      - ➢ Objekt podsítě lze přiřadit jen jednomu místu, ale jedno místo může zahrnovat více podístí.
   d. Potvrďte vytvoření podsítě pomocí OK

6. Prozkoumejte nastavení týkající se místní (*intrasite*) replikace
   a. Vyberte místo **Default-First-Site-Name** a v kontejneru Servers najděte server **w2016-dc**
   b. Pod serverem **w2016-dc** vyberte NTDS Settings a z kontextové nabídky otevřete jeho vlastnosti (Properties)
   c. Prozkoumete záložku Connections
   d. Pod serverem **w2016-dc** vyberte NTDS Settings a všimněte si objektů **příchozích** replikačních spojení.
   e. Z kontextové nabídky objektu spojení otevřete vlastnosti (Properties) a prozkoumejte záložku General.
7. Projděte si nastavení mezimístní (*intersite*) replikace pod kontejnerem Inter-Site Transports.
   - Lze použít dva protokoly pro mezimístní replikaci – **DS-RPC** (kontejner IP) a **ISM-SMTP** (kontejner SMTP).
8. Z kontextové nabídky objektu linky (*site link object*) **DEFAULTIPSITELINK** (pod kontejnerem IP) otevřete vlastnosti (Properties).
   a. Na záložce General naleznete i parametr Cost určující „cenu“ linky, potřebnou pro výpočet replikačních topologií.
   b. Objekt linky může zahrnovat i více míst.
9. Z kontextové nabídky kontejneru IP otevřete vlastnosti (Properties) a na záložce General si všimněte možnosti možnost Bridge all site links, která zapíná a vypíná tranzitivitu objektů linek.
10. Vytvořte objekt linky s názvem **BRNO** v kontejneru IP zahrnující místo **Default-First-Site-Link**.
    a. Z kontextové nabídky kontejneru IP zvolte New Site Link …
       - V tuto chvíli máme jen jedno místo, proto se zobrazí upozornění – přečtěte si jej a pokračujte OK
    b. Pojmenujte objekt linky **BRNO**
    c. Zkontrolujte, že zahrnuje místo **Default-First-Site-Name**
    d. a pokračujte OK

Lab X03 – 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** se přihlaste jako uživatel **administrator** do domény **testing.local**
2. Na **w2016-dc** otevřete **ADSS** (*Active Directory Sites and Services*)
   a. Start → Administrative Tools → **Active Directory Sites and Services**
3. 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

4. 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
5. 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
6. Přesuňte **w2016-repl** do místa **VUT** podle postupu z **bodu 5**
7. Vytvořte místo **FIT**, vypněte v něm automatické generování místní a mezimístní replikační topologie a přesuňte do něj server **w2016-base** podle postupů z **bodů 3 - 5**
8. 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
9. 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…
      - ✓ Upozorněte, že pod NTDS Settings jsou zobrazeny příchozí spojení a tedy při vytváření spojení vybíráme NTDS Settings cílového řadiče domény
   b. Ze Search result vyberte **w2016-dc** a zvolte OK
      - ✓ Řekněte, že zde volíme zase zdrojový řadič domény (tedy replikačního partnera)
   c. Jako název (Name) zadejte **dc2repl** a vytvořte objekt spojení pomocí OK
10. 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
11. 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
12. 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
13. Promítněte změny do replikační topologie **Active Directory**
    a. Na všech řadičích domény spusťte jako administrátor příkaz **repadmin /kcc**

14. Na **w2016-dc** proveďte nějakou změnu v **Active Directory** databázi, například u uživatele **homer** změňte hodnotu atributu Description
15. Zjistěte, na které řadiče domény byla změna replikována
    - ✓ Description se v **ADUC** zobrazí opožděně, je lepší otevřít vlastnosti objektu

    a. Ověřte, že na **w2016-repl** byla změna replikována
       - ✓ Pozor kam se připojí **ADUC** konzole, viz upozornění níže u **RODC**
       - ➢ 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 nové spojení z **w2016-repl** zpět na **w2016-dc** s názvem **repl2dc** podle postupu z **bodu 9**
20. Replikujte změny v konfiguraci na ostatní řadiče domény a promítněte je do replikační topologie podle postupů z **bodů 12 - 13**
21. Ověřte, že změny byly replikovány na **w2016-dc**

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 obě místa **VUT** a **FIT**

1. Na **w2016-dc** se přihlaste jako uživatel **administrator** do domény **testing.local**
2. Otevřete **ADSS** (*Active Directory Sites and Services*)
   a. Start → Administrative Tools → **Active Directory Sites and Services**
3. 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
4. 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**
5. 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
6. Nastavte **w2016-dc** jako **ISTG** pro místo **FIT** a povolte pro toto místo generování místní a mezimístní replikační topologie podle postupu z **bodů 4 – 5**
7. 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
8. 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. Po přečtení potvrďte pomocí OK
   c. Opakujte **body a – b** pro uzel **w2016-repl**
9. 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
      - Pokud došlo k vygenerování replikační topologie z **w2016-repl** směrem k **w2016-dc**, použijte v místě **VUT** k editaci ADSS připojené k serveru **w2016-repl** (alternativně bude potřeba po jednotlivých změnách potřeba použít Replicate configuration to the selected DC).
10. 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

11. 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**
12. Vraťte se zpátky na **w2016-dc** (resp. **w2016-repl**) 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
13. Nastavte **w2016-repl** jako upřednostňovaný bridgehead server pro místo **VUT** podle postupu z **bodu 7.a**
14. Přegenerujte mezimístní replikační topologii mezi místy **FIT** a **VUT** podle postupu z **bodu 10**
15. Na **w2016-base** ověřte, že bylo vytvořeno spojení z **w2016-repl** do **w2016-base**
    - Pokud spojení nebylo vytvořeno, proveďte postup z **bodu 10** na **w2016-base**