

Serverové systémy Microsoft Windows

IW2/XMW2 2018/2019

Peter Solár

solar@pocitacoveskoleni.cz

Fakulta Informačních Technologií
Vysoké Učení Technické v Brně
Božetěchova 2, 612 66 Brno

Revize 18. 3. 2019

Active Directory

Replikace

Replikace

- **Přesun dat** mezi **řadiči domény** (v doméně i lese)
 - Zajišťuje **dostupnost dat** potřebných pro fungování **Active Directory** (autentizaci, vyhledávání, ...)
- Probíhá tzv. *pull* metodou
 - **Stahování dat** z okolních řadičů domény
- Řeší dva základní problémy
 - **Výběr dat**, jenž mají být přesunuta
 - Výběr na úrovni **oddílů** databáze Active Directory
 - **Zjištění** (nejvhodnější) **cesty** pro přesun dat
 - Zjištění na základě **topologie sítě** Active Directory

Místa (*Sites*)

- Oblasti vyznačující se **dobrou konektivitou**
 - Většinou odpovídají fyzickým umístěním (budova, ...)
- Definovány **rozsahy** jedné nebo více **(pod)sítí**
 - Rozsahy reprezentovány **objekty podsítí** (*subnets*)
- Reprezentovány **objekty míst** (*site objects*)
 - Uloženy v kontejneru **Sites** v oddílu konfigurace
- Určují **průběh replikace**
 - Tvoří hranici mezi **místní** a **mezimístní** replikací
- Slouží k **lokalizaci služeb**

Vytvoření (objektu) podsítě

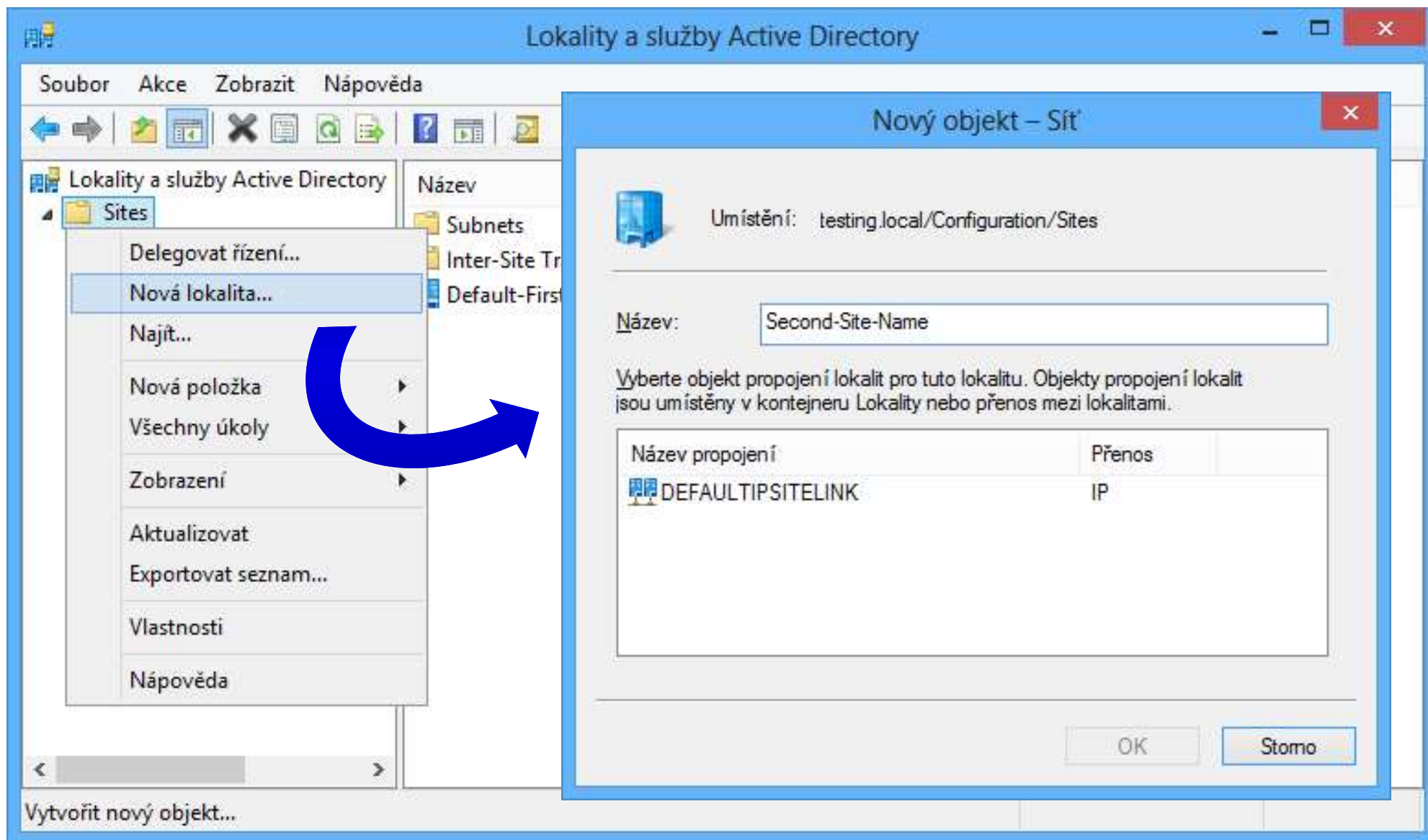
The image illustrates the steps to create a new subnetwork in Windows Server 2008 R2. On the left, the 'Lokality' console shows the 'Subnets' folder selected, with a context menu open. The 'Nová podsít...' option is highlighted. A blue arrow points from this option to the 'Nový objekt – Podsít' dialog box on the right.

The 'Nový objekt – Podsít' dialog box contains the following information:

- Umístění:** testing.local/Configuration/Sites/Subnets
- Zadejte pomocí zápisu síťových předpon (adresa/délka předpony) předponu adresy, kde délka předpony označuje počet pevných bitů. Můžete zadat předponu podsítě IPv4 nebo IPv6.**
 - [Další informace o zadávání předpon adres](#)
 - Příklad formátu IPv4:** 157.54.208.0/20
 - Příklad formátu IPv6:** 3FFE:FFFF:0:C000::/64
- Předpona:** 192.168.2.0/24
- Název předpony ve službě Active Directory Domain Services:** 192.168.2.0/24
- Vyberte pro tuto předponu objekt lokality.**
 - Název lokality:** Default-First-Site-Name

Buttons at the bottom of the dialog include 'OK', 'Storno', and 'Nápověda'.

Vytvoření (objektu) místa



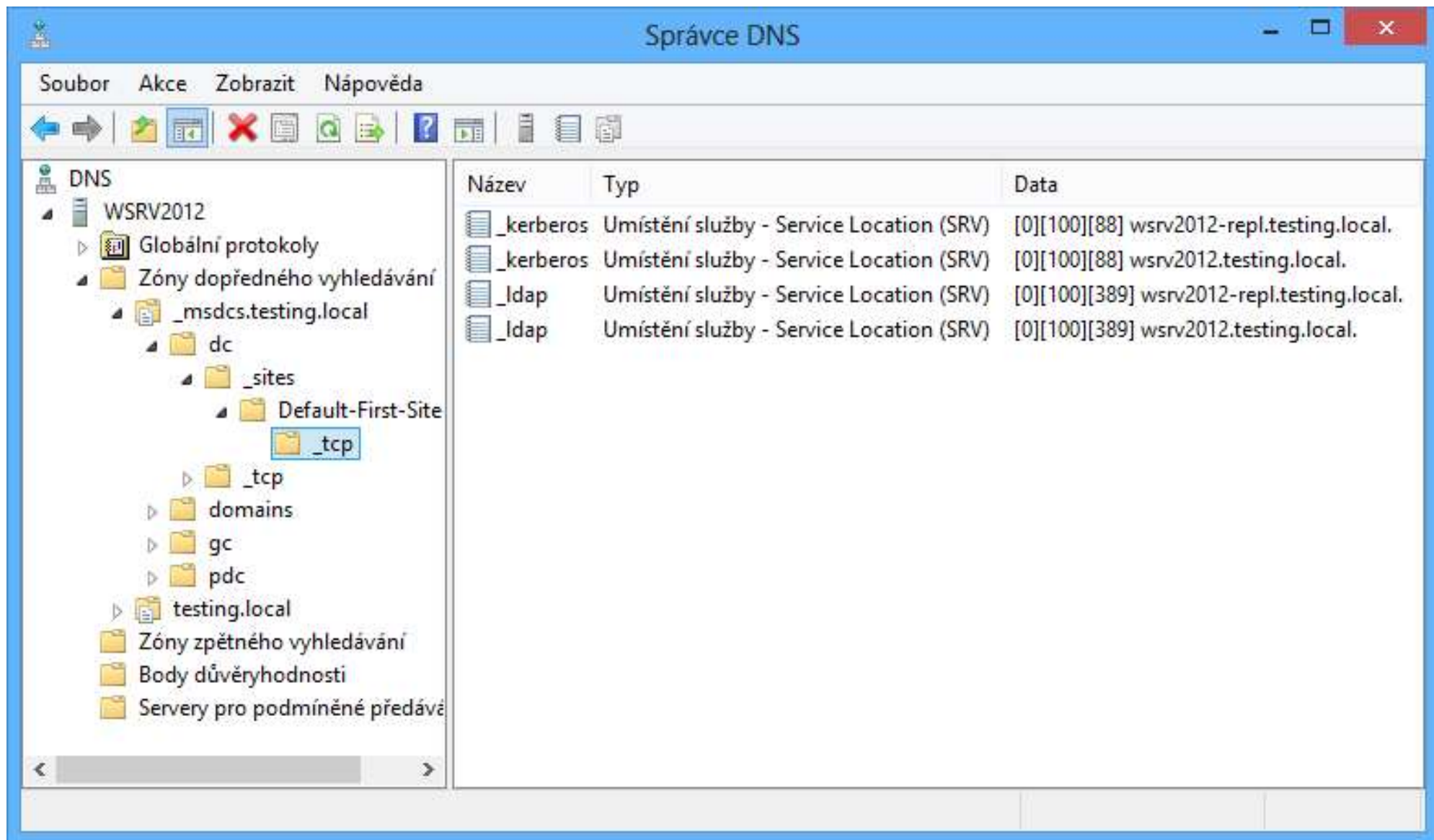
Správa replikačního provozu

- *Highly connected* síť (síť **uvnitř** míst)
 - Rychlá **konektivita**
 - Vysoká **propustnost**
 - Replikace prováděna **okamžitě** (ihned po změně)
 - Dokončení replikace v rámci sekund
- *Less highly connected* síť (síť **mezi** místy)
 - **Pomalá** nebo **nespolehlivá** spojení
 - Replikace prováděna v definovaných intervalech
 - **Plánování replikace** na konkrétní dobu

Lokalizace služeb

- Výběr **nejbližšího** serveru, jenž může **poskytnout** klientovi (počítači) požadovanou **službu**
 - Výběr serveru, jenž patří to **stejného** místa jako klient
- Probíhá na základě **SRV** záznamů **systemu DNS**
 - Překládají názvy **služeb** na doménová jména **serverů**, jenž tyto služby poskytují
 - Každý **SRV** záznam obsahuje
 - **Název služby** a **port**, na kterém služba naslouchá
 - Transportní **protokol**, který služba využívá (TCP nebo UDP)
 - Doménový **název poskytovatele** služby (serveru)

Uložení informací o službách v DNS



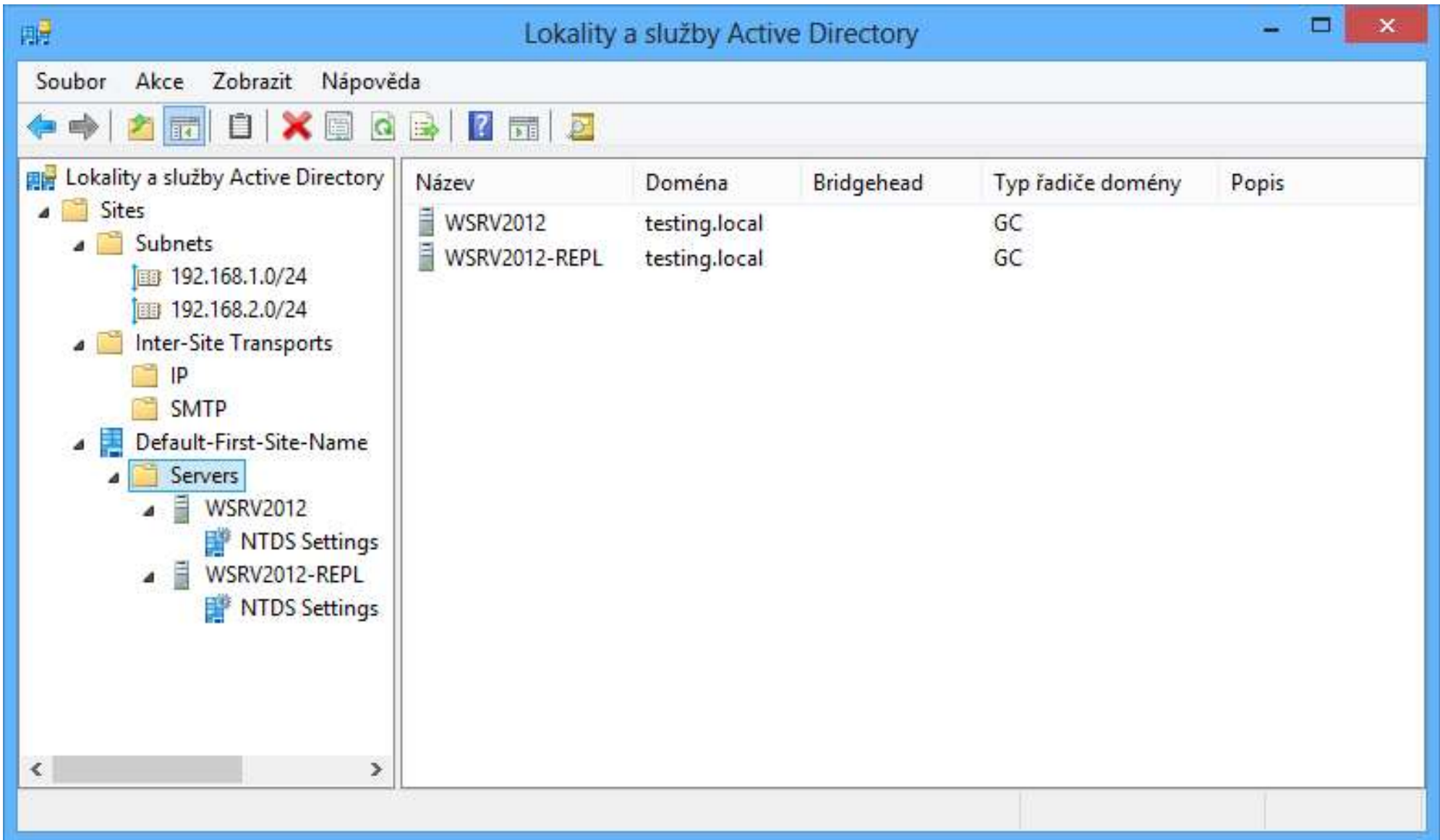
The screenshot shows the DNS Manager console for a server named WSRV2012. The left pane displays the tree structure of the DNS zones, with the following path selected: DNS > WSRV2012 > Zóny dopředného vyhledávání > _msdcs.testing.local > dc > _sites > Default-First-Site > _tcp. The right pane displays a list of SRV records for the selected zone.

Název	Typ	Data
_kerberos	Umístění služby - Service Location (SRV)	[0][100][88] wsrv2012-repl.testing.local.
_kerberos	Umístění služby - Service Location (SRV)	[0][100][88] wsrv2012.testing.local.
_ldap	Umístění služby - Service Location (SRV)	[0][100][389] wsrv2012-repl.testing.local.
_ldap	Umístění služby - Service Location (SRV)	[0][100][389] wsrv2012.testing.local.

Lokalizace řadičů domény

- Řadiče domény přiřazovány do míst **explicitně**
 - Přiřazení je **nezávislé** na IP adresách řadiče domény
 - Řeší problém **nejednoznačnosti** přiřazení, pokud má řadič domény přiřazeno **více** IP adres
 - **Výchozí** místo řadiče domény (místo, kde je umístěn po vytvoření) je vybráno na základě jeho **IP adresy**
 - První řadič domény v novém lese je automaticky umístěn do místa **Default-First-Site-Name**
- **Lokalizace** na základě **SRV** záznamů **systemu DNS**
 - **_kerberos** (autentizace) a **_ldap** (adresářové služby)

Umístění řadičů domény do míst



The screenshot shows the 'Lokality a služby Active Directory' (Active Directory Sites and Services) console. The left pane displays a tree view with the following structure:

- Lokality a služby Active Directory
 - Sites
 - Subnets
 - 192.168.1.0/24
 - 192.168.2.0/24
 - Inter-Site Transports
 - IP
 - SMTP
 - Default-First-Site-Name
 - Servers
 - WSRV2012
 - NTDS Settings
 - WSRV2012-REPL
 - NTDS Settings

The right pane displays a table of domain controllers:

Název	Doména	Bridgehead	Typ řadiče domény	Popis
WSRV2012	testing.local		GC	
WSRV2012-REPL	testing.local		GC	

Klíčové vlastnosti replikace AD (1)

- **Rozdělení** úložiště dat (na **oddíly**)
 - Replikují se pouze data z **vybraných** oddílů
 - **Minimalizace** množství přenášených dat
 - Lze vytvářet **vlastní** oddíly, tzv. **oddíly aplikací**
 - Obsahují objekty využívané aplikacemi nebo službami, jenž nepatří mezi základní (*core*) služby Active Directory
 - Nemohou obsahovat **identity** (*security principals*)
 - **Správa** pomocí nástroje **ntdsutil** (**create / delete nc**)
- **Adaptace** na podmínky okolní sítě
 - Odlišný průběh replikace v rámci místa a mezi místy

Klíčové vlastnosti replikace AD (2)

- **Automatické** vytváření **replikační topologie**
 - Dynamické (znovu)vytváření cest pro přenos dat
- Replikace na úrovni **atributů**
 - Přenáší se jen atributy objektů změněné od **poslední** replikace (**inkrementální** přenos dat)
- **Detekce** a řešení **kolizí**
 - **Algoritmy** pro řešení **různých** konfliktů při paralelních změnách atributů stejných objektů
 - Pokud **nelze** kolizi nijak **vyřešit**, pak je konfliktní verze objektu přesunuta do kontejneru **LostAndFound**

Spojení, replikační partneři a cesty

- **Spojení** (*Connection*)
 - Reprezentují **konektivitu** mezi dvěma řadiči domény
 - Vždy **jednosměrná** a to v **příchozím** (*inbound*) směru
- **Replikační partner** (*Replication Partner*)
 - Existuje-li spojení z řadiče domény **A** do **B**, pak řadič domény **A** je replikačním partnerem **B**
- **Replikační cesta** (*Replication Path*)
 - **Posloupnost** navazujících (sousedících) **spojení** mezi dvěma řadiči domény

Vytvoření (objektu) spojení

The screenshot shows the 'Lokality a služby Active Directory' console. The left pane shows the tree structure: Sites > Servers > WSRV2012 > NTDS Settings. A context menu is open over 'NTDS Settings', with 'Nové připojení služby Active Directory' highlighted. A blue arrow points from this menu item to the search dialog.

The search dialog, titled 'Najít – Řadiče domény služby Active Directory', contains the following text:

Řadiče domény služby Active Directory

V následujícím seznamu vyberte podle názvu nebo lokality řadič domény služby Active Directory.

(Seznam aktualizujte kliknutím na tlačítko Najít nebo zvolením příkazu Aktualizovat v nabídce Zobrazit.)

Buttons: Najít, Zastavit, Vymazat vše, OK

Search results table:

Název serveru	Síť	Doména
WSRV2012-REPL	Default-First-Site-Name	testing.local
WSRV2012	Default-First-Site-Name	testing.local

Počet nalezených položek: 2

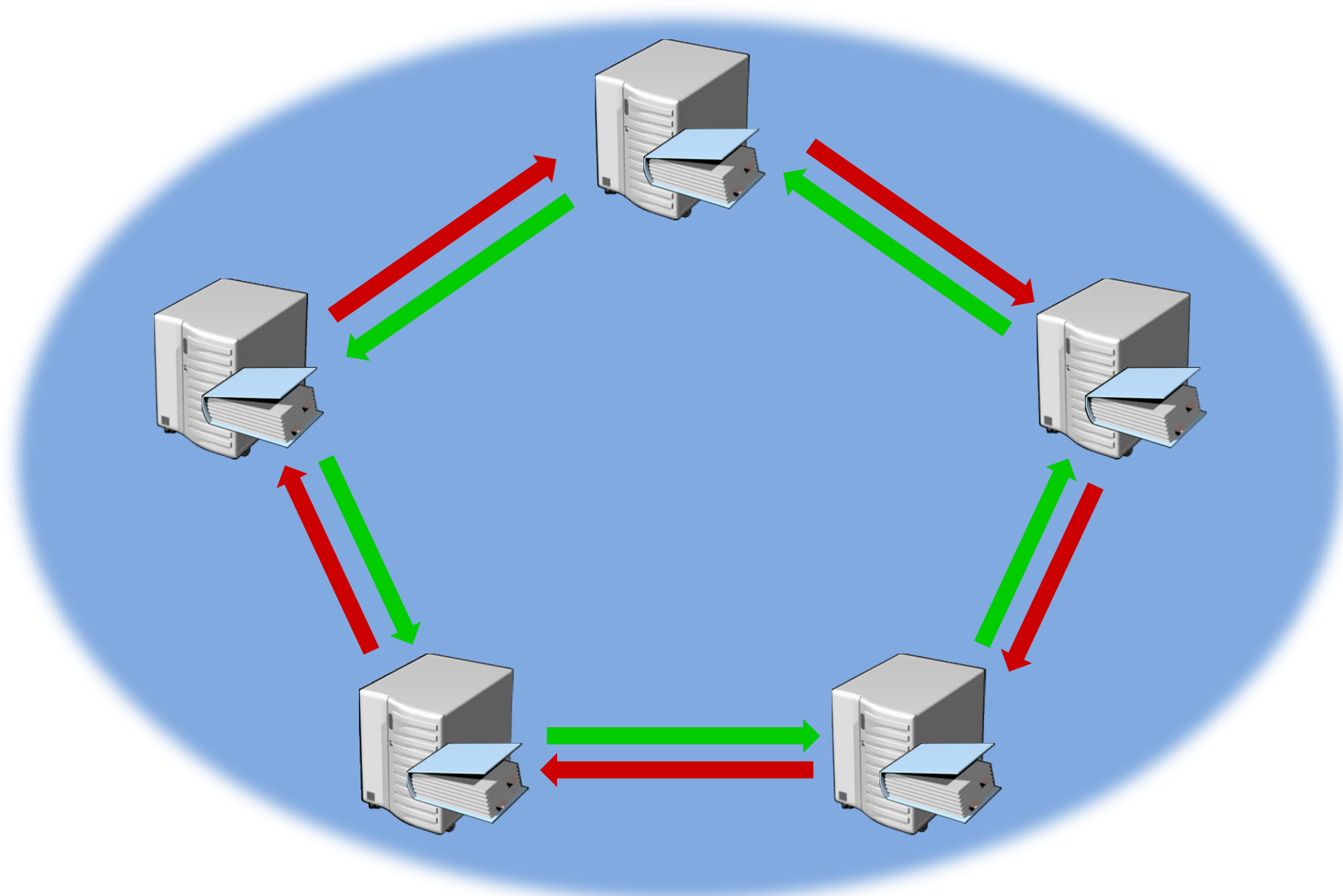
Replikační topologie

- **Množina** všech možných **replikačních cest**
 - Definuje **jak** přenést data mezi **dvěma** řadiči domény (přes které řadiče domény musí přenos probíhat)
- Určuje **replikační partnery** *pull* metody replikace
 - Stahování dat od replikačních partnerů
- Vytváření zajišťuje komponenta Active Directory **KCC** (*Knowledge Consistency Checker*)
 - Automaticky **vytváří** potřebné (objekty) **spojení**
 - Spojení lze vytvářet i **manuálně** (jsou **perzistentní**)

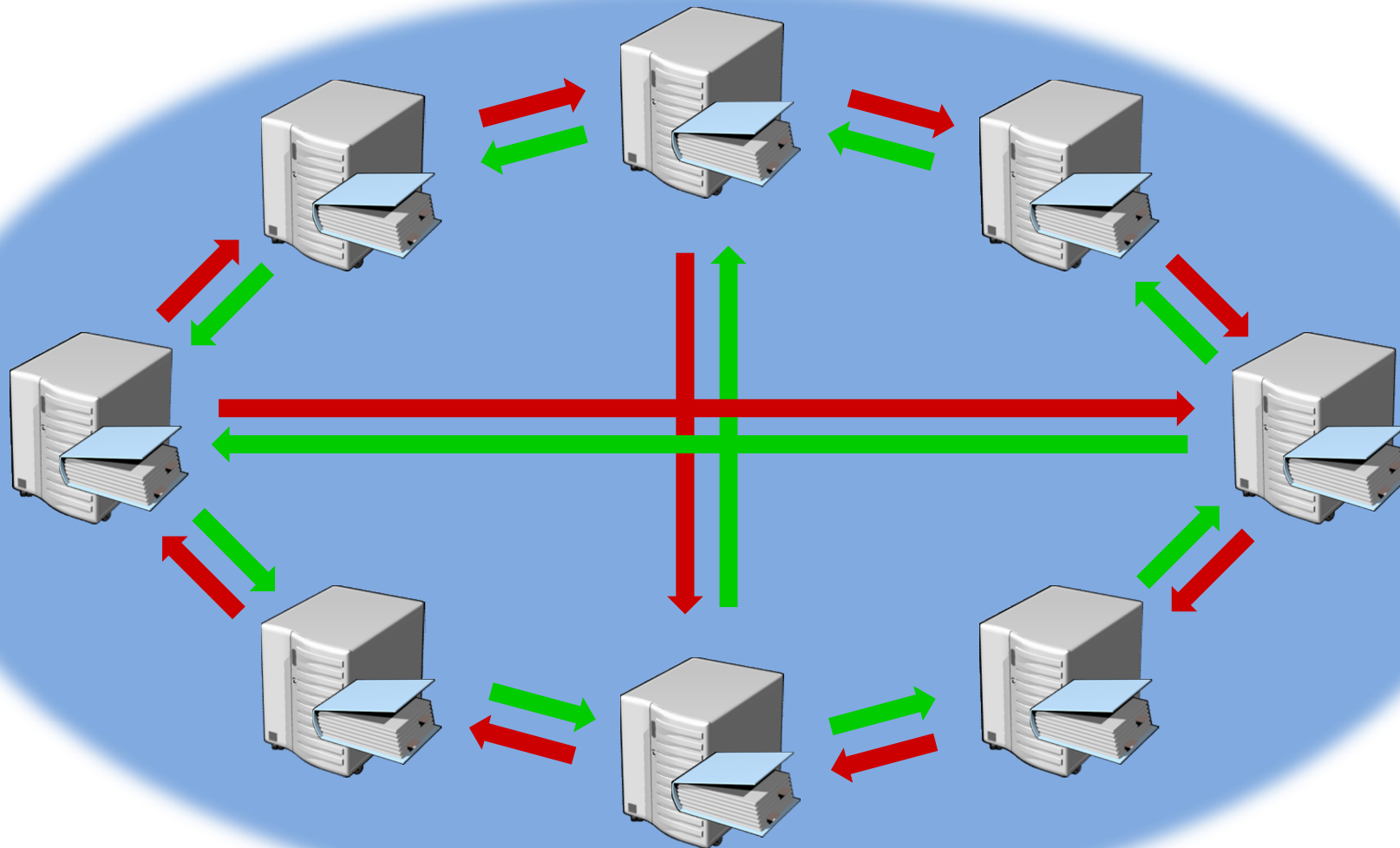
Generovaná replikační topologie

- **Dvoucestná** topologie
 - Vždy existují alespoň 2 **rozdílné** replikační cesty mezi dvěma řadiči domény
- Maximální počet **tří skoků**
 - Mezi dvěma řadiči domény musí existovat replikační cesta o maximální délce 3
- 2 **typy** vytvářených topologií
 - **Kruh** (*ring*) v případě **malého** počtu řadičů domény
 - **Mřížka** (*mesh*) pro **větší** počet řadičů domény

Topologie typu kruh (*ring*)



Topologie typu mřížka (*mesh*)



Místní (*intrasite*) replikace

- Replikace změn v rámci jediného **místa**
 - **Rychlý** přenos změn v databázi Active Directory
- Každé dva **řadiče domény** jsou **sítově dostupné**
 - Každý řadič domény může komunikovat s kterýmkoliv jiným řadičem domény v daném místě
 - **Ignoruje** se (fyzická) topologie sítě
- 2 možnosti iniciace replikace
 - **Oznámení** (*notification*)
 - **Vyzývání** (*polling*)

Oznámení (*notification*)

- Zasílá **zdrojový** řadič domény (**replikační partner**) po provedení změny v některém svém oddílu AD
 - Po uplynutí 15 sekund **prvnímu** řadiči domény, který má zdrojový řadič jako svého replikačního partnera
 - Každé 3 sekundy **dalšímu** (cílovému) řadiči domény
- Po přijetí oznámení řadič domény spustí **replikaci**
 - Realizuje **agent replikace adresáře** (DRA)
 - Po **dokončení** replikace se řadič sám stává **zdrojovým** řidičem domény a celý proces oznámení se opakuje
 - Replikace změn na všechny řadiče domény v rámci minut

Vyzývání (*polling*)

- **Dotazování** se replikačních partnerů na **změny**
 - Provádí cílový řadič domény co 1 hodinu (lze změnit)
 - Pokud došlo ke **změnám**, je provedena **replikace**
- Při **selhání** (replikační partner neodpovídá) dojde k ověření **replikační topologie** pomocí **KCC**
 - Ověření **dostupnosti** všech **replikačních partnerů**
 - Umožňuje dynamicky **měnit** replikační topologii když je **nedostupný** (selže) některý z **řadičů domény**

Nastavení intervalu vyzývání

<Vygenerováno automaticky> – vlastnosti

Obecné Objekt Zabezpečení Editor atributů

<Vygenerováno automaticky>

Popis:

Změnit plán...

Zdroj replikace

Server: WSRV2012-REPL

Server: Default-First-Site-Name

Replikované názvové kontexty: ForestDnsZones.testing.io

Částečně replikované názvové kontexty: Všechny další domény

OK Stomo Použít Nápověda

Plán uživatele <Vygenerováno automaticky>

0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0

Vše

pondělí

úterý

středa

čtvrtek

pátek

sobota

neděle

pondělí až neděle od 0:00 do 0:00

OK

Stomo

Nikdy

Jednou za hodinu

Dvakrát za hodinu

Čtyřikrát za hodinu

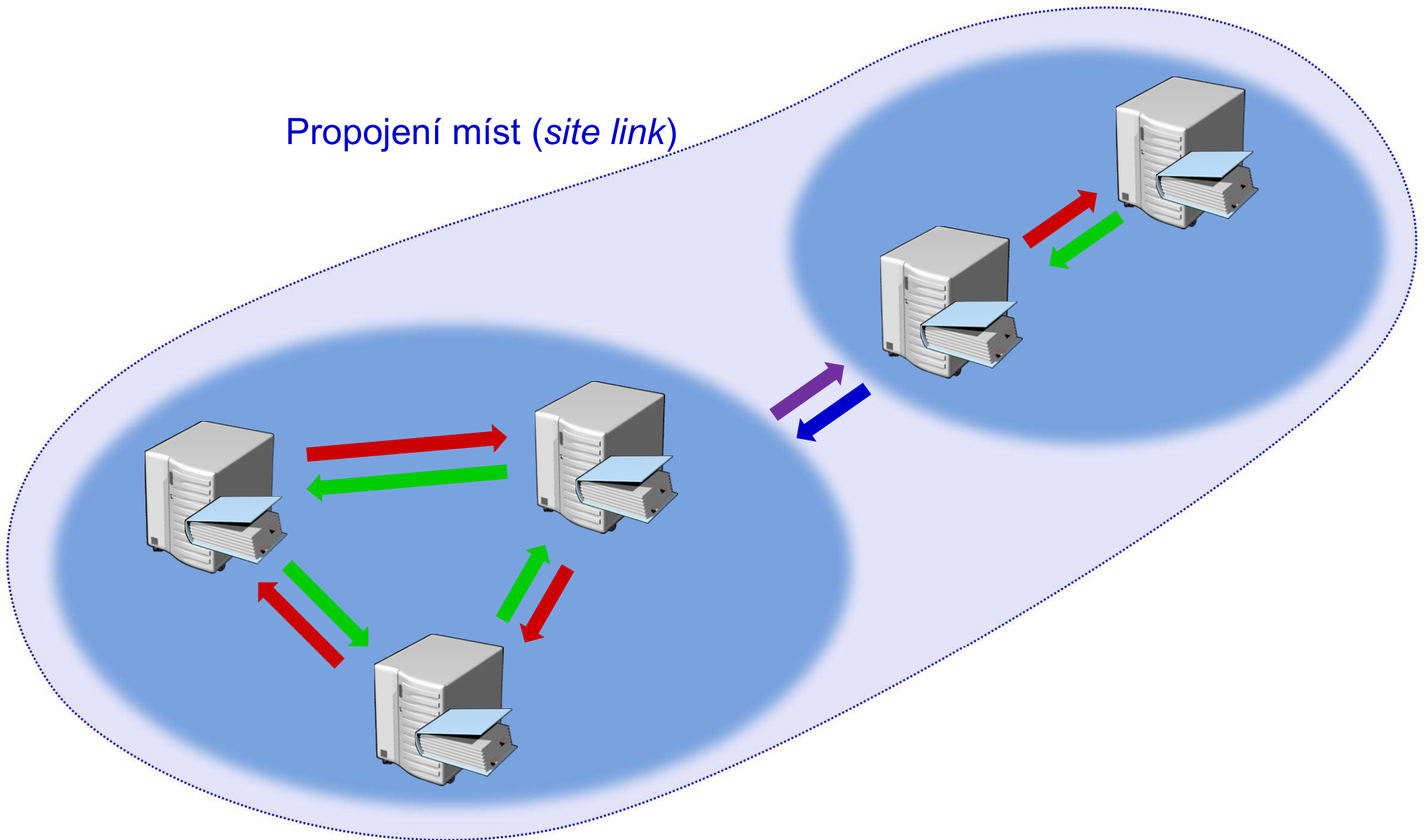
- Nastavuje se pro každého replikačního partnera (spojení) **zvlášť**

Mezimístní (*intersite*) replikace

- Replikační topologii vytváří **generátor mezimístní topologie** (ISTG, *Intersite Topology Generator*)
 - Generuje (objekty) **spojení** na základě **propojení míst**
- **Propojení míst** (*site link*)
 - Reprezentuje síťovou konektivitu mezi **místy**
 - Může zahrnovat dva nebo více míst (*sites*)
 - Vytvářeny vždy **manuálně**

Ilustrace propojení míst

Propojení míst (*site link*)



Vytvoření (objektu) propojení míst

The screenshot displays the 'Lokality a služby Active Directory' (Active Directory Sites and Services) console. The left pane shows the hierarchy: Sites > Subnets > 192.168.1.0/24 > IP. A context menu is open over the 'IP' folder, with 'Nové propojení lokalit...' (New inter-site link...) selected. A blue arrow points from this menu item to the 'Nový objekt – Spojení sítí' (New object – Network connection) dialog box.

The dialog box 'Nový objekt – Spojení sítí' is open, showing the following configuration:

- Umístění: testing.local/Configuration/Sites/Inter-Site Tr
- Název: SECONDIPSITELINK
- Lokality neobsažené v tomto propojení lokalit: (Empty list)
- Lokality obsažené v tomto propojení lokalit: Default-First-Site-Name, Second-Site-Name
- Buttons: Přidat >>, << Odebrat
- Message: Propojení lokalit musí obsahovat alespoň dvě lokality.
- Buttons: OK, Storno

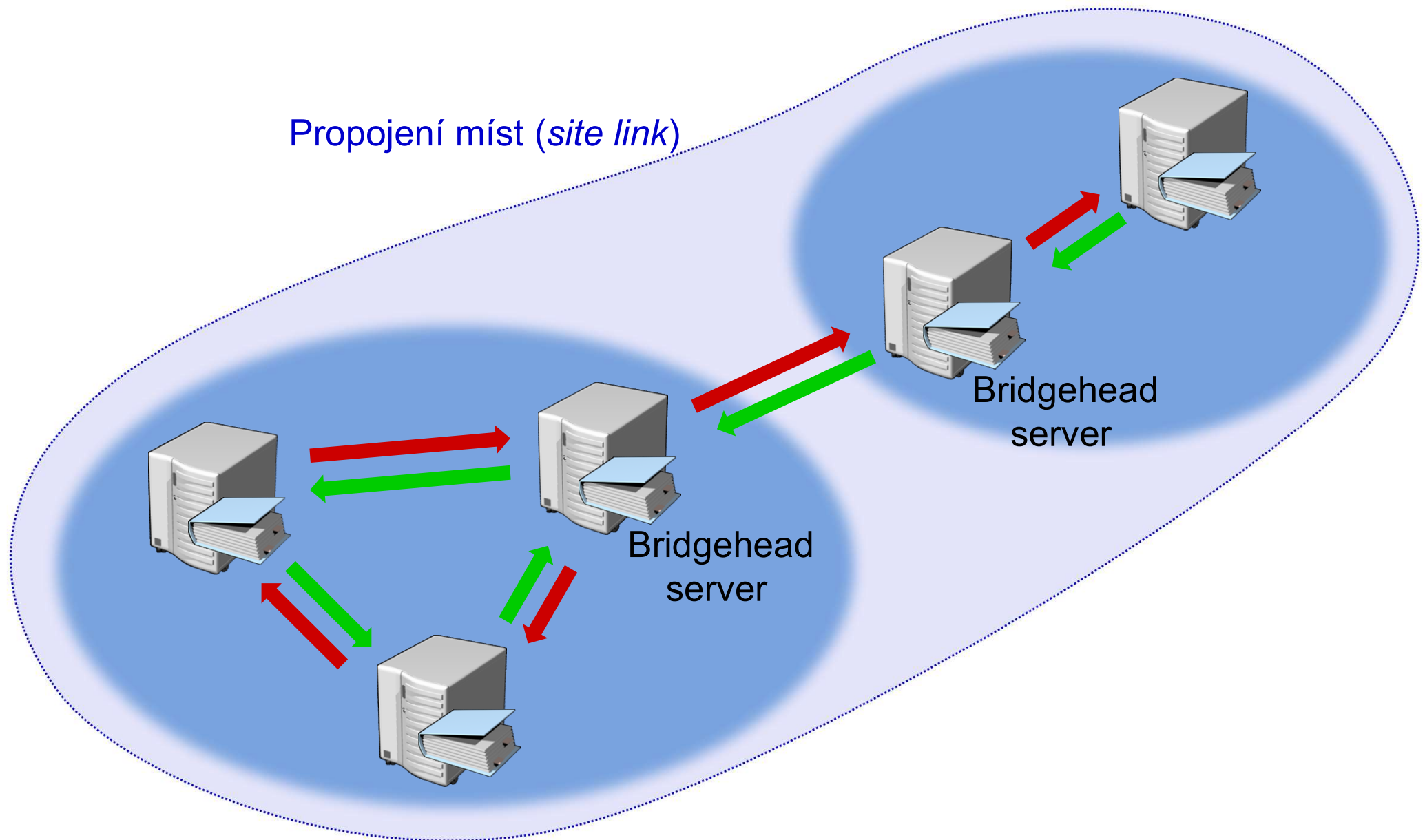
Protokoly pro přenos (replikaci) dat

- **DS-RPC** (*Directory Service RPC*)
 - **Jediný** protokol pro **místní** replikaci
 - **Upřednostňovaný** protokol pro **mezimístní** replikaci
 - Může replikovat **oddíl domény** (*domain partition*)
- **ISM-SMTP** (*Inter-Site Messaging SMTP*)
 - **Nemůže** replikovat **oddíl domény**
 - Vyžaduje přítomnost **certifikační autority** (CA)
 - **Robustnější** (využíván při **nespolehlivém** spojení mezi místy, pokud tato místa nenáleží do stejné domény)

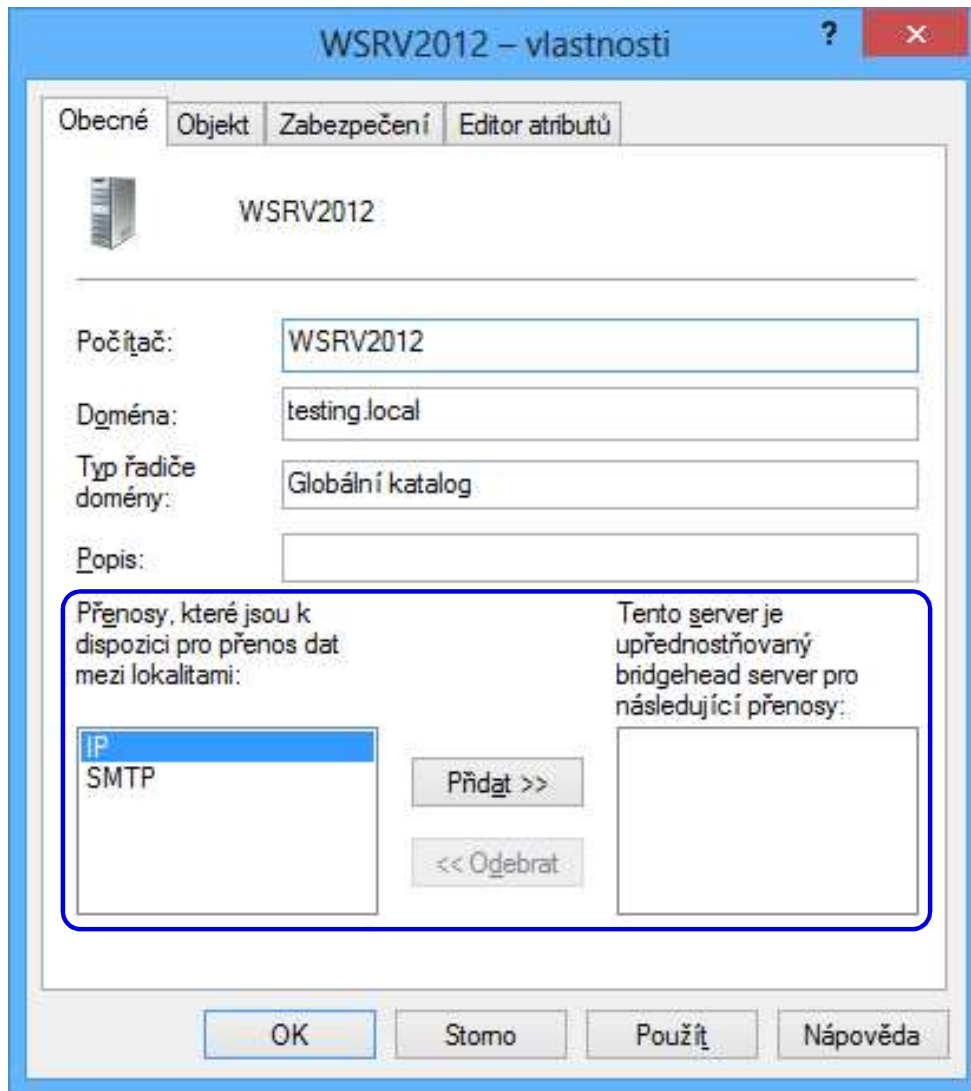
Bridgehead servery

- Řadiče domény, jenž zajišťují **mezimístní replikaci vybraných oddílů** databáze Active Directory
 - V každém místě existuje jeden **bridgehead server** pro **každý oddíl** databáze Active Directory
- Lze **explicitně vybrat** preferované řadiče domény, jenž by měly plnit úlohu **bridgehead serverů**
 - Při výpadku přesun na jiný **preferovaný** řadič domény
- **Minimalizují přenos** dat mezi jednotlivými místy
 - Data se přenášejí pouze **jednou** mezi každou dvojicí míst v daném (objektu) propojení míst

Ilustrace bridgehead serverů



Preferované bridgehead servery

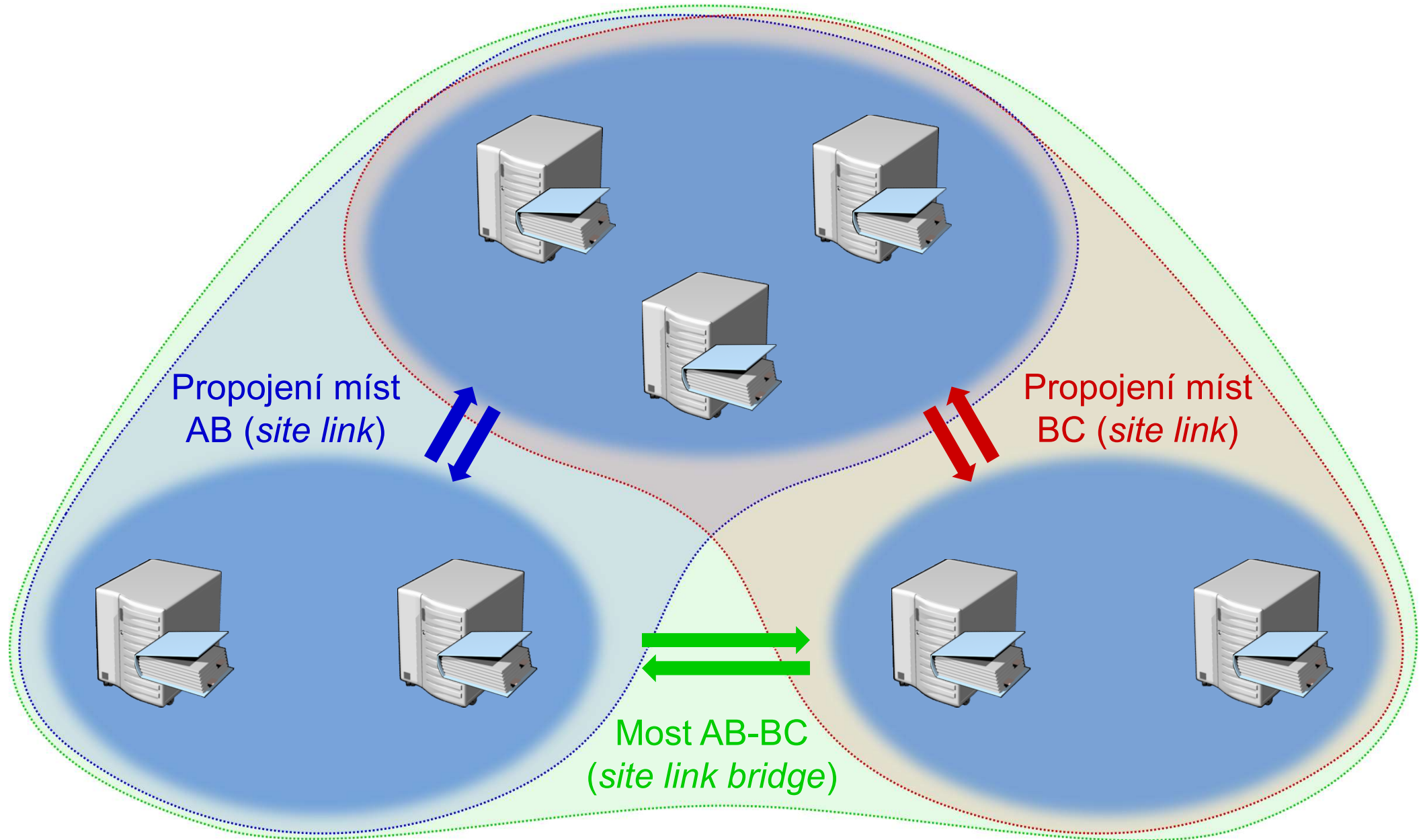


- Vždy pouze pro určitý **typ** transportního **protokolu**
- Pokud není **žádný** z řadičů domény preferován, jsou automaticky preferovány **všechny** přítomné řadiče
- V případě **nedostupnosti** všech preferovaných řadičů domény **selže** **mezimístní** replikace

Nastavení mezimístní replikace

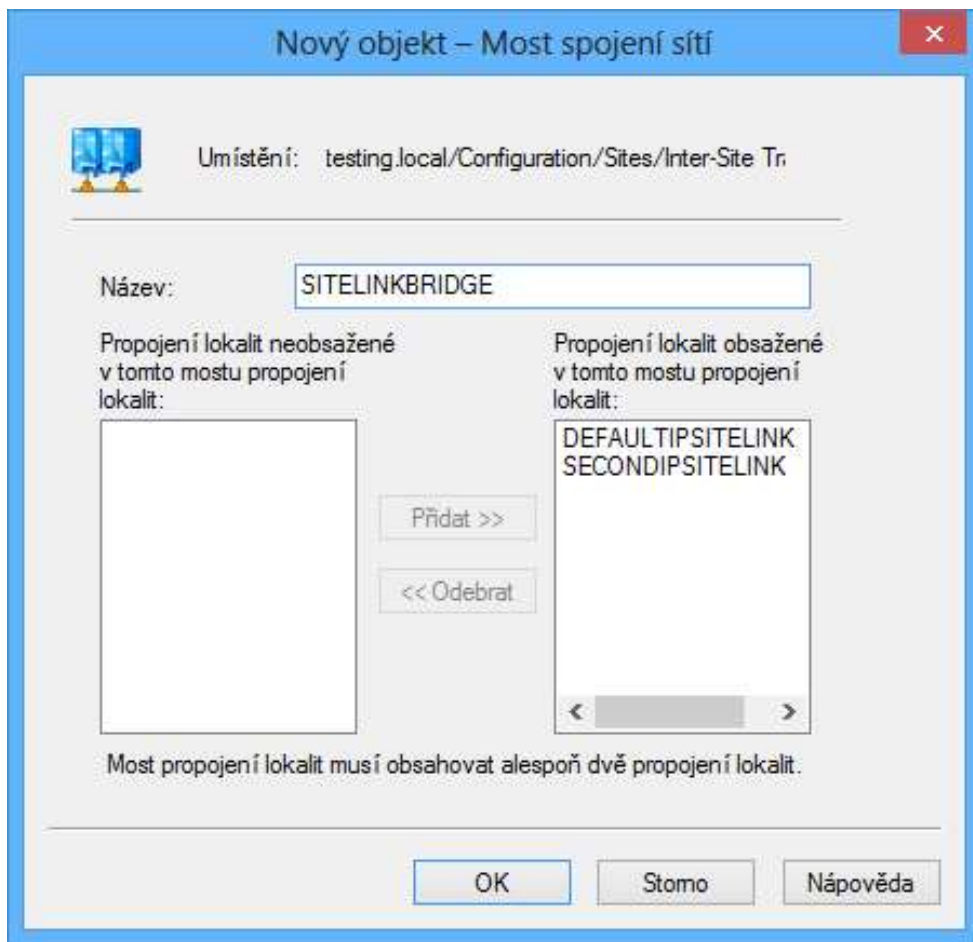
- **Tranzitivita (objektů) propojení míst**
 - Pokud lze provést replikaci mezi dvojicemi míst **A** a **B** a **B** a **C**, pak lze provést replikaci také mezi **A** a **C**
 - Ve výchozím nastavení **povolena**
- **Mosty (objektů) propojení míst (*site link bridges*)**
 - Spojení dvou a více (objektů) propojení míst, které vytváří jedno **tranzitivní** propojení míst
 - Pokud je povolena **tranzitivita propojení míst**, jsou **ignorovány**

Ilustrace mostů propojení míst

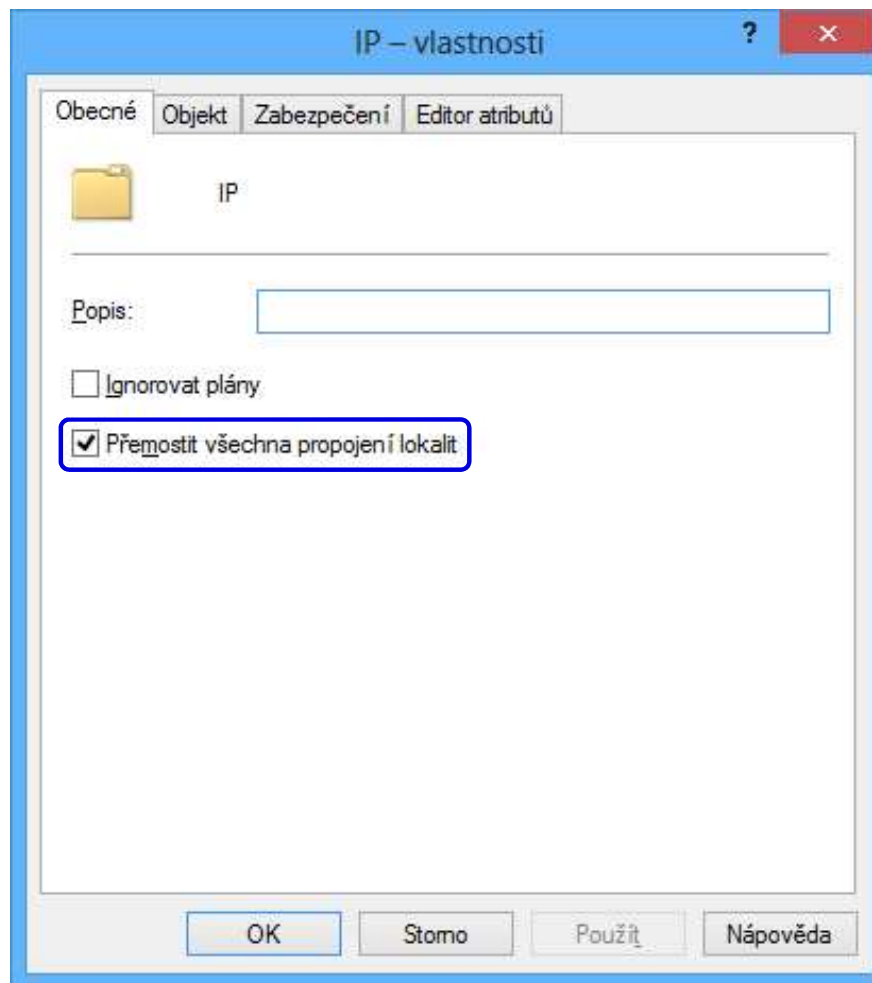


Vytváření mostů propojení míst

Manuálně



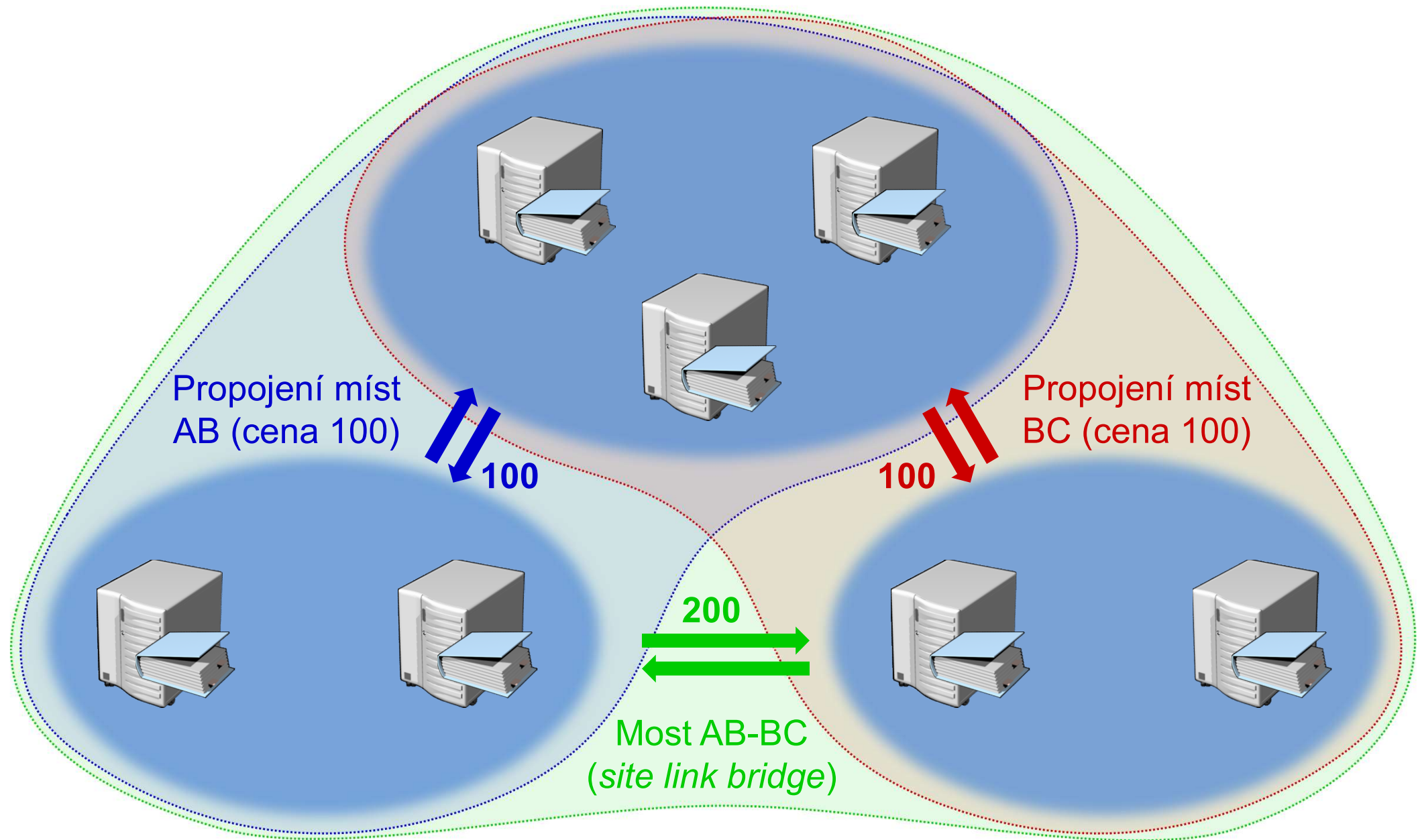
Automaticky (tranzitivita)



Cena replikačních cest

- **Cena (objektů) propojení míst** (*site link cost*)
 - Určuje **pořadí výběru** replikační cesty, pokud existuje **více** možných **cest** mezi dvěma **řadiči domény**
 - Ve výchozím nastavení mají všechna propojení míst cenu 100
- **Cena replikační cesty**
 - **Součet cen** propojení míst, přes které replikační cesta prochází
 - Čím **nižší** cena, tím **více** bude cesta **preferována** před ostatními cestami

Ilustrace cen replikačních cest



Plánování mezimístní replikace

- **Frekvence replikace** (*frequency*)
 - Mezimístní replikace založena výhradně na **vyzývání**
 - **Interval dotazování** se **bridgehead serverů**, zda u nich nedošlo k nějakým **změnám**
- **Plánování replikace** (*schedule*)
 - Možnost **omezení replikace** na určité hodiny
 - Ve výchozím nastavení může být replikace provedena **vždy** (povolena 24 hodin denně)

Nastavení ceny, frekvence a plánu

DEFAULTIPSITELINK – vlastnosti

Obecné Objekt Zabezpečení Editor atributů

DEFAULTIPSITELINK

Popis:

Lokality neobsažené v tomto propojení lokalit:

Lokality obsažené v tomto propojení lokalit:

Přidat >>

<< Odebrat

Náklady: 100

Replikovat vždy po 180 minutách

Změnit plán...

OK Stomo Použít Nápověda

Plán uživatele DEFAULTIPSITELINK

0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0

Vše

pondělí

úterý

středa

čtvrtek

pátek

sobota

neděle

pondělí až neděle od 0:00 do 0:00

OK

Stomo

Replikace není k dispozici

Replikace je k dispozici

- Plán určuje, kdy je možné mezimístní replikaci přes propojení míst provádět

Nástroj repadmin.exe

- Výpis replikačních partnerů / (objektů) spojení
 - `repadmin /showrepl <dc-list>`
 - `repadmin /showconn <dc-list>`
- Spuštění KCC (aktualizace replikační topologie)
 - `repadmin /kcc`
- Spuštění replikace mezi dvěma řadiči domény
 - `repadmin /replicate <dest-dc-list> <src-dc> <nc>`
- Synchronizace se všemi replikačními partnery
 - `repadmin /syncall <dc> /A /e`

Výpis seznamu replikačních partnerů

```
Správce: Příkazový řádek repadmin /showrepl win2008r2-dc

DC-testing,DC-local
  Second-Site-Name\WIN2008R2-REPL přes RPC
  Identifikátor GUID objektu agenta DSA: 664a2856-e213-4cf2-8aef-e27acaee6a21

  Poslední pokus z 2011-03-20 22:52:08 byl úspěšný.

CN-Configuration,DC-testing,DC-local
  Second-Site-Name\WIN2008R2-REPL přes RPC
  Identifikátor GUID objektu agenta DSA: 664a2856-e213-4cf2-8aef-e27acaee6a21

  Poslední pokus z 2011-03-20 22:52:08 byl úspěšný.

CN-Schema,CN-Configuration,DC-testing,DC-local
  Second-Site-Name\WIN2008R2-REPL přes RPC
  Identifikátor GUID objektu agenta DSA: 664a2856-e213-4cf2-8aef-e27acaee6a21

  Poslední pokus z 2011-03-20 22:52:08 byl úspěšný.

DC-DomainDnsZones,DC-testing,DC-local
  Second-Site-Name\WIN2008R2-REPL přes RPC
  Identifikátor GUID objektu agenta DSA: 664a2856-e213-4cf2-8aef-e27acaee6a21

  Poslední pokus z 2011-03-20 22:52:08 byl úspěšný.

DC-ForestDnsZones,DC-testing,DC-local
  Second-Site-Name\WIN2008R2-REPL přes RPC
  Identifikátor GUID objektu agenta DSA: 664a2856-e213-4cf2-8aef-e27acaee6a21

  Poslední pokus z 2011-03-20 22:52:08 byl úspěšný.
```

Nástroj dcdiag.exe

- Provádí **testování** funkčnosti **doménových služeb Active Directory (AD DS)**
 - **Spuštění** testu příkazem **dcdiag /test:<název-testu>**

Název testu	Popis testu
FrsEvent	Zjišťuje chyby služby replikace souborů (FRS)
DFSREvent	Zjišťuje chyby replikace distribuovaného souborového systému (DFS-R)
Intersite	Zjišťuje problémy ovlivňující provádění mezimístní replikace
KccEvent	Zjišťuje chyby komponenty KCC
Replications	Kontroluje včasnou replikaci mezi řadiči domény
Topology	Kontroluje, zda replikační topologie zahrnuje všechny řadiče domény
VerifyReplicas	Ověří replikaci oddílů aplikací na řadiče domény, jenž je mají obsahovat