Topologie

Šimon Suchomel

Úkoly

- Nainstalujeme 2. řadič domény
- Povolíme DNS, jinak žádné role
- Po instalaci se mrkneme na DNS Forwarders – nastavíme Brno

Sites

- Překládáno jako síť, nejedná se o fyzickou síť
- AD sites a site links, nemusí odpovídat topologii fyzických sítí
- Site je „oblast“, site link je cesta, site musí mít site link

- Slouží k:
  - Řízení replikačního provozu
  - Usnadnění rozmístění služeb

Sites plánování

- Př.:
  - 2 vzdálené lokace, 1DC v každé lokaci, jsou spojené rychlou sítí, rozhodli jsme se pro 1 společnou site
  - Podnik v rámci velkého dobře zasíťovaného kampusu, chceme vést uživatele k užívání zdrojů v jejich budově, rozhodli jsme se pro více site kvůli prioritizaci lokálních služeb
- Typicky spojují lokace s „dobrým“ síťovým spojením
- Rozmístění služeb – př. DC, DFS
- Koncentrace uživatelů

Sites plánování

- Vytvoření nové site v případě:
  - Část sítě je spojená pomalým připojením
  - V síti je lokace, kde je dost uživatelů pro vynucení hostování služeb v té lokaci
  - Provoz sítě si vynucuje „lokální“ DC
  - Chceme řídit lokalizaci služeb
  - Chceme řídit replikaci mezi DC

Subnet

- Objekt typu subnet definuje rozsah IP adres
- Je spojený s objektem typu site
- Lokalizace služeb probíhá tak, že se IP adresa stroje spojí s danou site pomocí vztahu mezi objekty site a subnet
- Site může mít více subnets
- Subnet může být asociována pouze k 1 site
- Př. 10.10.10.0/24
- Vždy definujte všechny fyzické podsítě jako objekty AD subnet

Úkoly

- Přejmenujeme defaultní site na Headquarters
- Vytvoříme subnety 10.10.10.0/24 a 10.10.15.0/24 pro defaultní site
- Vytvoříme novou site DolniRakousko
- Vytvoříme novou subnet 10.10.11.0/24 pro Dolní Rakousko
- Vytvoříme novou site BratislavskyKraj
- Vytvoříme novou subnet 10.10.12.0/24 pro Bratislavský kraj

Kontrolní otázka

- Klientký počítač, který je umístěn ve vzdálené pobočce P, je pomalý během přihlašovacího procesu. Všimli jste si, že počítač hlásí, že jeho logon server je DC ve vzdálené site místo DC v site v rámci pobočky P. Co z následujícího může být zdrojem potíží:
  A. DC na pobočce P nemá přiřazenou site
  B. Site na pobočce P není v žádném site link
  C. Rozsah IP adres pobočky P není asociovaný s danou site
  D. Subnet pro pobočku P je přiřazena pro 2 site

Active Directory Partitions

- Domain partition
  - Všechny doménové objekty (uživatelé, skupiny, počítače, Group Policy Containers), repl. Na DC v rámci domény
- Configuration partition
  - Objekty reprezentující logickou strukturu lesa a topologii (domény, sites, subnets), repl. na všechny DC v lese
- Schema partition
  - Třídy a atributy objektů, repl. na všechny DC v lese
- => ntds.dit
- GC nese tzv. Patrial attribute set (ze všech domén)
- Application directory partition
  - Obsahuje objekty pro aplikace či služby mimo jádra AD DS, může být replikováno na specifické řadiče, př. DNS Active Directory Integrated Zone

Úkoly

- Prohlédnem si Application Directory Partition
  - ADSI Editor, WK Naming Context vyberem *Configuration* a proklikáme se k partitions
  - Všimneme si *Directory Partition Name* doménové DNS zóny
  - Přepojíme ADSI Editor a zadáme DN jméno do pole pro DN
  - Proklikáme se k záznamům DNS

DCs in sites

- Kdy spravovat DC v sites:
  - Když přidáme novou site a přesouváme existující DC
  - Když rušíme DC
  - Když instalujeme nové DC
- Site Coverage – pro site bez DC
- SRV záznamy v DNS

Úkoly

- Změníme síťovou konfiguraci:
  - Serveru 1 – Brno – přidáme 2 další IP adresy k LAN rozhraní, 10.10.11.1/24 a 10.10.12.1/24
  - Serveru 2 – Vídeň – nastavíme IP 10.10.11.2/24
  - Serveru 3 – Bratislava – nastavíme IP 10.10.12.2/24
- Přesuneme Vídeň do Dolního Rakouska

Replikace

- Dělení data store. NC v rámci domény
- Automatické generování replikační topologie
- Attribute-level Replication
- Oddělené řízení intrasite a intersite replikace
- Detekce kolizí

Replikace

- Objekty typu Connection
  - jednocestné
- KCC
- Intrasite Replication
  - Notifikace – server se změnou počká 15 sekund na initial notification, potom 3 sekundy na subsequent notification
  - Replikační topologie o maximálně 3 skocích
  - Replikace dokončená během 1 minuty
  - Polling – jednou za hodinu

Intersite Replikace

- Pomocí objektů site links
  - Reprezentuje dostupnou cestu pro replikaci
  - Obsahuje 2 a více Site
  - ISTG (InterSite Topology Generator) buduje spojení mezi servery, součást KCC

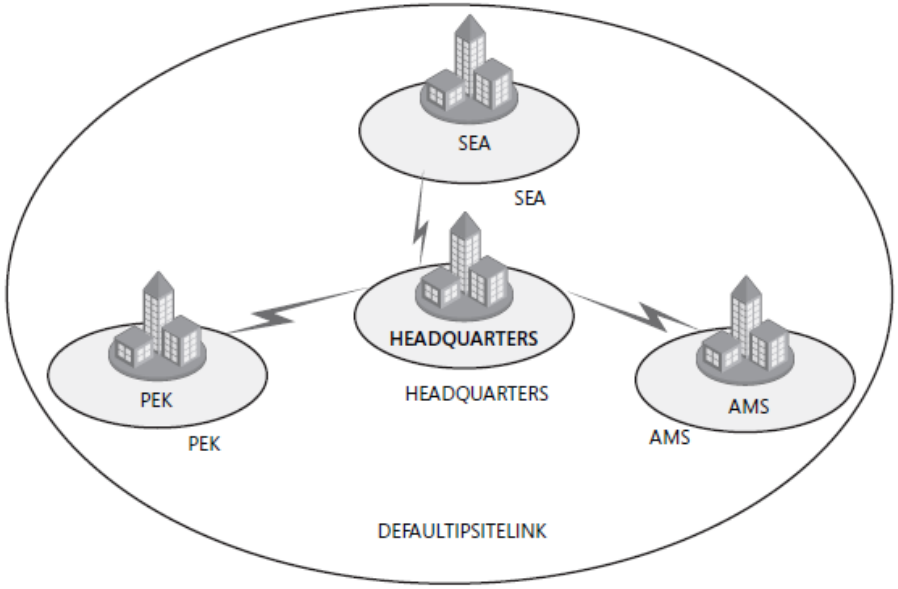

Figure 11-11 Network topology and a single site link

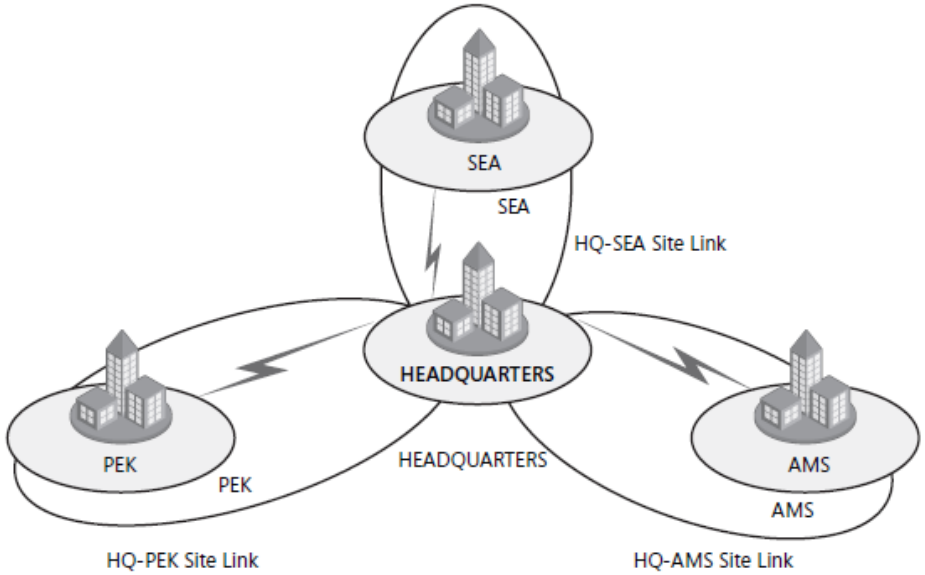

Figure 11-12 Network topology and a three-site link

Převzato z MCTS Self Paced Training Kit Exam 70-640.Configuring Windows Server 2008 Active Directory

Bridgehead servers

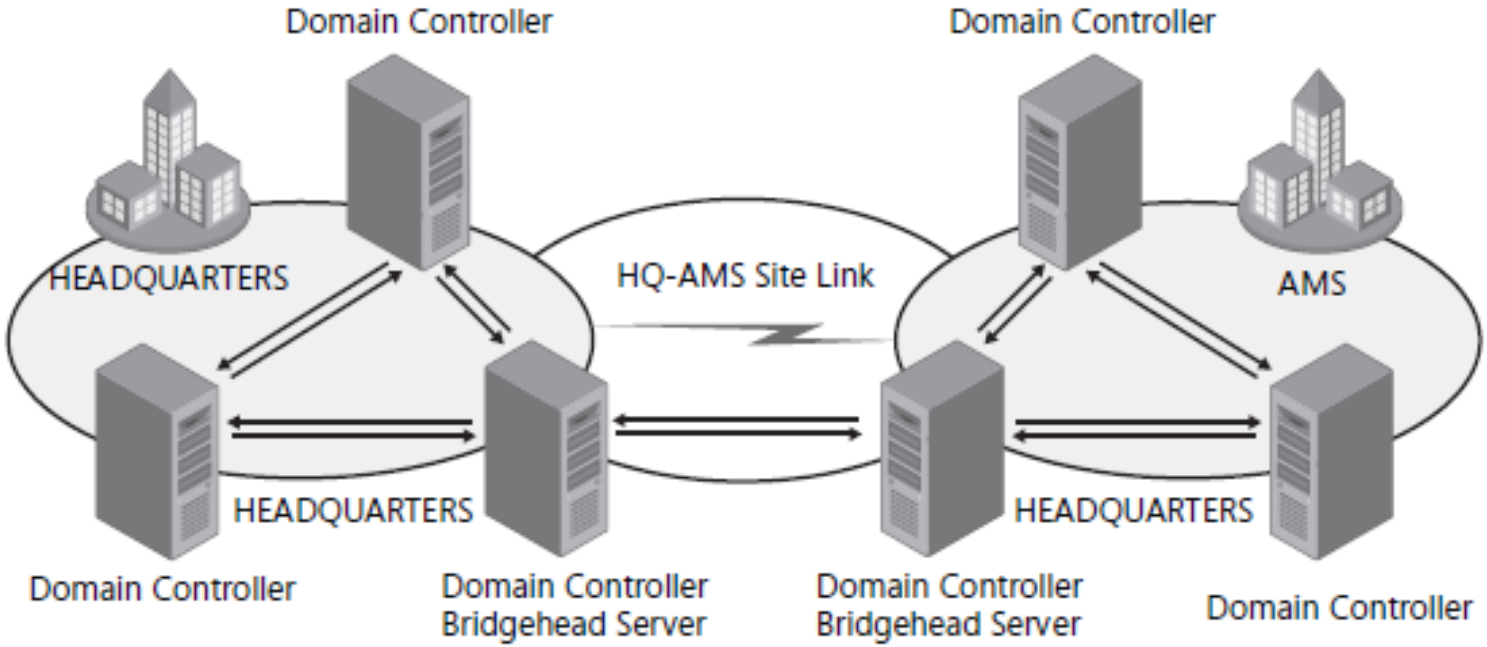

Figure 11-13 Sites, intrasite replication, bridgehead servers, and intersite replication

- Lze nakonfigurovat preferované bridgehead servery
  - Může ji být více
  - Z důvodu výkonnosti
  - Nastavení Firewall

Převzato z MCTS Self Paced Training Kit Exam 70-640.Configuring Windows Server 2008 Active Directory

Nástroje

- Repadmin
- Dcdiag

Úkoly

- Vytvoříme a zrušíme Connection Object z Brna do Vídně, Brno – Operations Master
- Přesuneme Infrastructure master. Je to k něčemu?
- Ve Vídni zapneme GC
- Přejmenujeme defaultní site link na HQ-Dolni_Rakousko, odstraníme z něj Bratislavský kraj
- Vytvoříme nový site link HQ-Bratislavský_kraj
- Zvolíme preferovaný Bridghead Server
  - ve vlastnostech serveru pod objektem Site
- Nastavíme častější replikaci mezi HQ a Vídní
- Nastavíme cenu na 300 mezi Brnem a Bratislavou
  - Oboje ve vlastnostech objektu Site Link
- Omrkneme transitivní linky ve vlastnostech Inter-Site transportního protokolu

Úkoly

- Nainstalujeme child doménu na serveru Bratislava
- Při instalaci zapneme DNS i GC
- Replikaci zvolíme ze serveru Brno
- Po restartu přidáme DNS forwarder na Brno
- Znovu restartujeme

Trusty

- Jedná se o Kerberos autentizaci
- Logické spojení mezi doménami umožňující přeposlanou autentizaci
- Vlastnosti:
  - Transitivní / netransitivní
  - Jednosměrné / obousměrné
  - Automatické / Manuální

Automatické trusty

- Transitivní
- Obousměrné
- Automatické

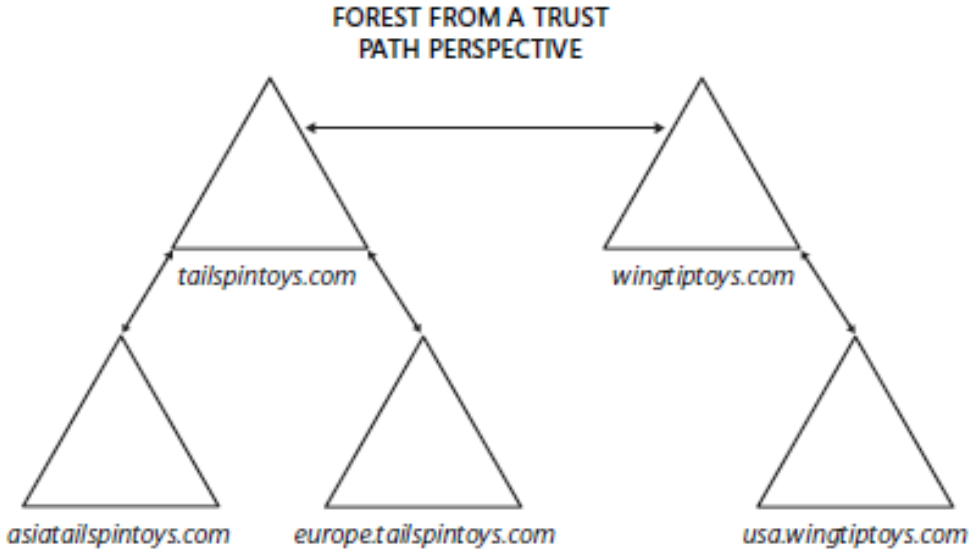

Figure 12-7 An Active Directory forest from a DNS perspective and from a trust path perspective

Převzato z MCTS Self Paced Training Kit Exam 70-640.Configuring Windows Server 2008 Active Directory

Manuální trusty

- Shorcuts – mezi doménamy v lese
- External Trusts – trust s doménou z jiného lesa
- Realm Trust – cross platform interoperabilita
- Forest Trust – trust mezi 2 nezávislými foresty

Úkoly

- Ověřte automatický trust v AD Domains and Trusts