Topologie

Šimon Suchomel

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

- Použití:
  - Řízení replikačního provozu
  - Autentizace
  - 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, fc00:a:a:cafe::/64
- Vždy definujte všechny fyzické podsítě jako objekty AD subnet

Kontrolní otázka

- Klientský 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

DCs in sites

- Úprava topologie = změna Configuration Partition = potřeba skupiny Enterprise Admin
- 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

Replikace

- Multimaster, Loose consistency, Convergence
- Store-and-forward replication
- Pull replication
- Automatické generování replikační topologie
- Oddělené řízení intrasite (vnitřní) a intersite (vnější = mezi site) replikace
- Detekce kolizí

Replikace

- na základě GUID, tzn. rozliší se nový objekt od změněného objektu se stejným DN
- Attribute-level Replication

Replikace – topologie

- Objekty typu Connection
  - jednocestné
- KCC
- Intrasite Replication
  - Notifikace – server se změnou počká 15 sekund na initial notification, další případné partnery notifikuje po 3 sekundách (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

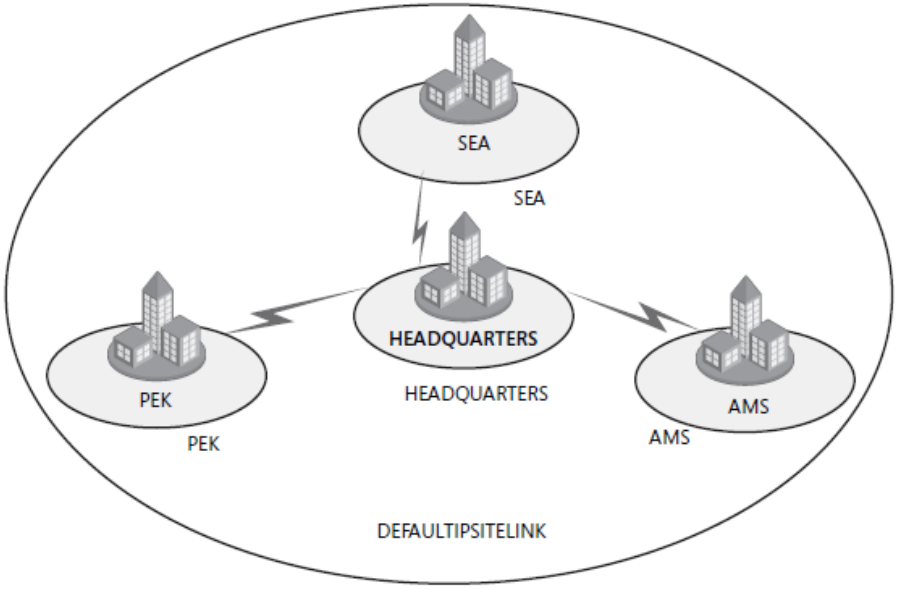


Figure 11-11 Network topology and a single site link

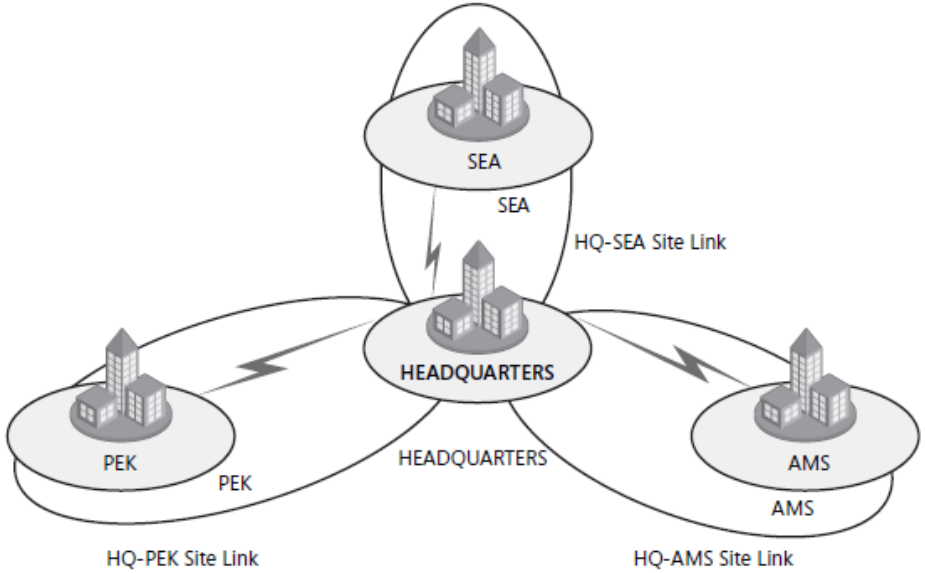
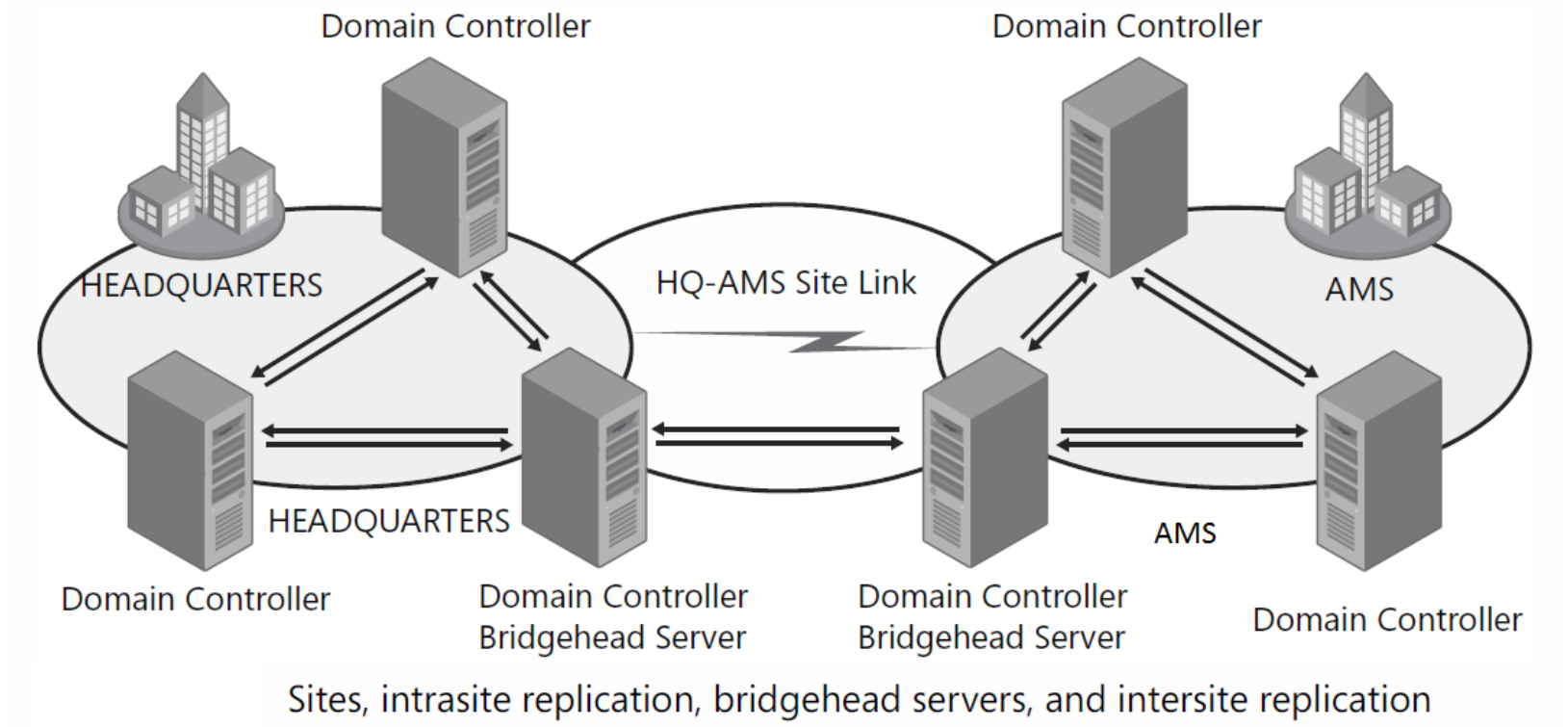


Figure 11-12 Network topology and a three-site link

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

Bridgehead servers



- Lze nakonfigurovat preferované bridgehead servery
  - Může jich 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
  - př. repadmin /showrepl
    repadmin /kcc
- dcdiag – diagnostický nástroj
- get-ADReplication* cmdletty
- př. get-ADReplicationFailure ad.local

Vícedoménové prostředí

- 1 doména:
  - Jediná domain partition na všech řadičích
  - Jediná politika pro Kerberos
  - Jediný DNS jmenný prostor
- Standardní doporučení zní: Les o jediné doméně.
- Les je bezpečnostní hranice.

Trusts = vztahy důvěry

- Jedná se o Kerberos autentizaci
- Uvnitř domény vs. mezi doménami
- Logické spojení mezi doménami umožňující přeposlanou autentizaci
- Vlastnosti:
  - Transitivní / Netransitivní
  - Jednosměrné / Obousměrné
  - Automatické / Manuální

Automatické

- Transitivní
- Obousměrné
- Parent-child trust

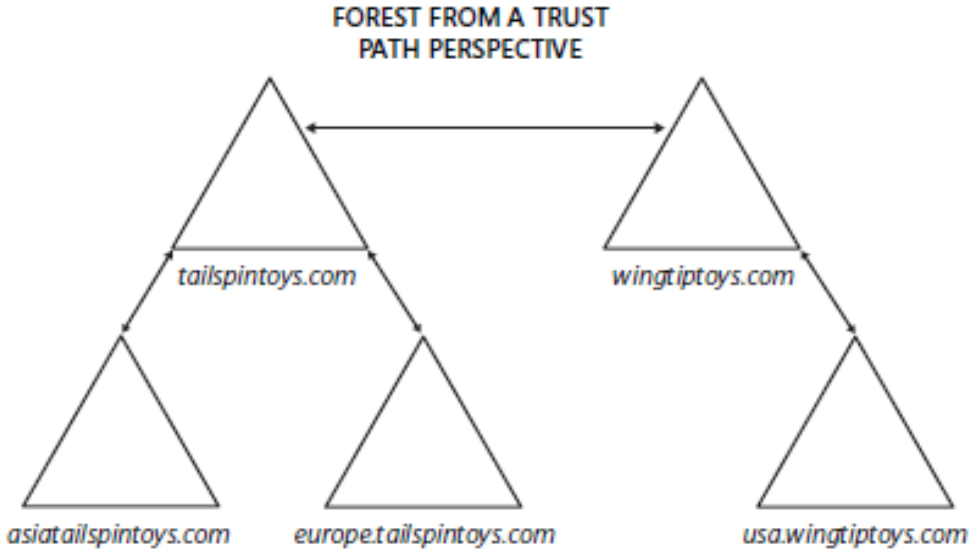


Figure 12-7 An Active Directory forest from a DNS perspective and from a trust path perspective

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

Manuální

- Shorcuts – mezi doménami v lese
- External Trusts – trust s doménou z jiného lesa
- Realm Trust – mezi platformní interoperabilita
- Forest Trust – trust mezi 2 nezávislými lesy