AD SITE

Každá active directory doména má minimálně 3 části(adsi editor – v něm jsou vidět):

1. **schéma** – zahrnuje informace popisující databázi, obsahuje třídy a atributy + informace které třídy používají které atributy. Schéma je stejné ve všech doménách lesa – replikuje se i mezi doménami. (mohou měnit pouze enterprise admins ci schéma admins)
2. **konfigurační** – zahrnuje informaci o konfiguraci. replikuje se i mezi doménami (mohou menit pouze enterprise admins). Zde jsou například objekty aktive Directory Site.
3. **doménová** – vytváření účtů, počítačů, GPO objekty, nástroj active directory users and computers – pracuje s doménovou částí. Replikuje se mezi všemi řadiči v rámci stejné domény, do ostatních nezasahuje.
4. **aplikační** část(od Windows 2003 nula až neomezeně defaultně po instalaci jsou 2) – slouží k nastavení replikace mezi konkrétními řadiči(i z jiných domén) k nastavení např. úložiště aplikací apod.

Replikace v **doménách NT4.0** 1 řadič PDC a ostatní BDC. Replikace topologie hvězda s PDC uprostřed. Vytváření objektů a celkově zápis byl pouze na PDC. BDC pouze pro čtení.

V **aktive directory** probíhá **MULTIMASTER replikace.** Replikuje každý s každým. Změny lze provádět kdekoliv. Replikační topologie se nastavuje automaticky(tak aby mezi 2ma náhodně vybranými řadiči nebylo více než 3 skoky). Vypadne-li řadič přegeneruje se topologie.

Replikační interval **závisí od** režimu **celého lesa**(domain functional level):

- windows 2000 mixed ci native – do 5 minut se replikuje mezi 2ma řadiči v rámci 1 site
- windows 2003 – do 15 sekund se replikuje mezi 2ma řadiči v rámci 1 site

Globální katalog

Je read-only databáze obsahující vybrané informace o všech objektech celého lesa. (ve schématu u atributu je zaškrtávátko že má byt v globálním katalogu). Globální katalogy se replikují dle konfigurace administrátorem.

Active directory site – reprezentují fyzické rozložení domény. Je-li linka pomalejší jak 500kbitů/s tak se nespouští skripty nelze nainstalovat software atd.(minimální rychlost závisí na GPO objektu). Proto je-li linka slabší jak 1,5mbit(T1) tak je lepší dát tam řadič. Ve výchozím nastavení je 1 site. Replikuje se v rámci 1 site. Mezi site lze nastavit libovolný čas replikace v rámci site nikoliv. Sites se vytvářejí v nástroji Ad sites and services(česky sítě a služby active directory).
Po vytvoření site je třeba přidělit řadič do site a nastavit **ip site transport**(defaultně 3 hodiny interval na replikaci, minimum je 15 minut max 10080 minut(1 týden)). Na ip site transport lze kromě intervalu také nastavit čas kdy(např. pouze večer). Lze natavit také cost spojeni. Používá se nejlevnější cesta(nejnižší cost). Lze nastavit i přes smyl replikaci (namisto IP), ale tato neumí replikovat doménovou část(lze tudíž využít jen mezi doménami). Na site lze nastavit GPO objekty co platí v celé site(moc se nepoužívá).

Průběh replikace

Replikace v **rámci site** probíhá tak, že má-li řadič co replikovat notifikuje ostatní a ti si to stáhnou jakmile jim doběhne 5 minut interval. Jakmile nejsou notifikováni nedělají nic. Data se nekomprimují.

Replikace **mezi site** se nenotifikuje jakmile uběhne interval řadič se zeptá druhého a ten buď řekne že nic nebo pošle. Data se komprimují.
Replikace probíhá na úrovni atributů – lze změnit 2 různé atributy na různých řadičích změny se nereplikují správně(pozor členství ve skupinách je jedním atributem ☺ jsou to typicky linked multiatribute položky).

Subnet – nastaví subnet adresy aby se počítače dané site ověřovali u řadiče v té dané site. Informace, který řadič obsluhuje kterou doménu jsou v DNS v srv záznamech.

Vynucení replikace – v nástroji AD sites and services proklikat na site na řadič a ntds – tam je seznam connection objektů a pravým na něj a replicate now(replikuje jen něco např. uživatele ano počítače ne – závisí na tom jestli jsou ze stejné site).

Nástroj ze support tools (rpmon) – replikační monitor – po spuštění přidat servery ke sledování. Replikace vypsány po částech, i s informací kdy a odkud apod.

Před replikací se řadiče vzájemně ověřují. Pokud replikace přestane fungovat a jeden počítač si změní heslo, tak se již neověří a replikace již nefunguje. Řešením je explicitně změnit heslo(nástrojem netdom reset pwd jako parametr server na kterém se to má zreplikovat) a znova nareplikovat změnu hesla.

Pokud jeden admin odstraní prázdnou OU ale jiný mezitím do ni něco strčí a ještě to není replikováno tak obsah najdete po replikaci v **losts and founds**(nutno zaškrtnout advanced features).

Bridgehead server – nastaví, že přes tento řadič se bude přednostně replikovat intersite replikace (nastavuje se ve vlastnostech serveru).

Jak udělat z řadiče Globální katalog – ad sites and services – pravým properties na ntds settings a zaškrtnout global katalog a počkat než se nareplikuje – až se nereplikuje pak se zobrazí jeho srv záznam v dns

V site by měl být řadič sity, globální katalog a DNS server – i při výpadku se pak uživatelé normálně přihlásí.

Universal group membership caching – funkce zastupuje globální katalog, protože má informace o členství v globálních skupinách (cache se obnovuje každých 8 hodin)
Lze nastavit na úrovni site – **ntds site settings(**neplést s ntds settings což je u každého řadiče**)**

Operation masters (FSMO)

5 rolí:

Schema master

- Spravuje schéma veškeré úpravy domény – prázdni atributu či objektu, vyber toho co bude v globálním katalogu a tak se dějí zde
- Nefunguje-li pak nepůjde upravit schéma

Domain naming master

- Stará se o to aby při přidávání podřízené domény bylo správně a neduplikátní jméno
- Nefunguje-li pak nepůjde přidat či odebrat podřízená doména

PDC emulator

Má 5 rolí:

1. Ověřuje uživatele – při změně hesla se tato změna okamžitě nastavuje zde a při přihlašování se ověřuje také zde(jinak by nemuselo byt ještě zreplikováno takže pokud zadá špatné heslo tak se řadič zeptá PDC emulatoru jestli heslo není náhodou novější)
2. Starší klienti (NT4.0 a starší windows) si mění heslo přímo na PDC emulátoru(lze obejít nainstalováním windows active directory client)
3. Je autoritativní server pro replikaci na doméně NT4.0(slouží jako PDC při replikaci)
4. Je časovým serverem v doméně (je-li rozdíl klient řadič v čase více než 5 minut nedojde k autorizaci klienta a nepřihlásí se). V doménách active directory u win 2000 a výše je automatická synchronizace času. Klient si synchronizuje čas s tím serverem, se kterým se na začátku ověřuje a potom se synchronizuje ten den jen s nim(defaultně každé 4 hodiny se synchronizuje čas, pokud je rozdíl více než xy tak se zkrátí interval na polovinu čili 2 hodiny). Také řadiče domény se synchronizuji s PDC emulátorem. PDC emulatory se synchronizuji s PDC v nadřazených doménách. Korenovy PDC (událost w32time v logu pokud tomu tak není) se většinou s externím(time.windows.com) ci lokálním časovým zdrojem.
5. Je serverem kde se ve výchozím nastaveni provádí úpravy GPO (group policy objektu) – všechny změny přes gpmc se provádí na PDC emulatoru – aby nedocházelo ke konfliktům při konfiguraci více správci zároveň

Nefunguje-li pak při okamžitém přihlášení po změně hesla to může byt problém(časem se na replikuje), časová synchronizace nefunguje a může se rozejit po určitém čase, editace GPO nelze dělat na PDC (lze na jiném řadiči) – v radu několika hodin není ztráta této role až tak vážná

RID(relative id) master

- Kód SID (jedinečný identifikátor uživatele lze najit v tokenu přes whoami /?) má část doménovou a část relative ID
- Při vytváření nového objektu(např user) se generuje na radici SID, RID master přiděluje skupiny relative ID jednotlivým řadičům(kvůli jedinečnosti)
- Nefunguje-li pak nějakou dobu lze normálně vytvářet objekty, ale jakmile dojdou řadiči jeho relative ID tak nemá možnost získat novou skupinu relative

ID a objekt nelze vytvořit(viz systémový log kde je napsáno ze nelze přidělit objektu relative ID)

Infrastructure master

- Duležitý v prostředí s více doménami (2 a více)
- Pokud jeden objekt jedné domény přiřadíme do druhé tak se tam vytvoří zástupce a když něco změníme na tom objektu jez je jinde zastupován tak infrastructure master zařídí změny ve všech zástupcích
- Zástupce pozná tak, že vezme databázi řadiče domény a globálního katalogu, co je navíc jsou objekty z cizích domén(zástupci) – z toho vyplývá, že infrastructure master ***nesmí*** být na řadiči, který je zároveň globální katalog – pak by to nefungovalo protože by porovnával globální katalog s globálním katalogem(neplatí ve 2 případech – existuje jen jedna doména nebo v případě ze každý řadič domény je globální katalog – práci infrastructure mastera pak nahrazuje replikace globálního katalogu)
- Nefunguje-li pak se změny nedistribuují a zástupci mají staré hodnoty

Jak zjistit který server je co: z příkazové řádky či klikátkem(adir users and computers - > pravý klik operations masters(zde je RID, infrastructure a PDC emulator)), domain naming master je v adir domains and trusts a schéma master je v adir schema(třeba doinstalovat (regsvr32 schmmgmt.dll) pak se objeví v MMC) tamtéž lze udělat transfer

Nejde li transfer pak je nutné udělat SEIZE: původní server je nutno již nepřipojit do site protože ten se nedozví že už nemá tuto roli. Seize se dělá výhradně na příkazovém řádku pomocí nástroje ntdsutil(nt directory services util). Velmi intuitivní nápověda přes help. Je nutné mít správně připojeno na požadovaný řadič.

Kam s kterou roli(doporučení):
Single domain forest – všechny role na prvním řadiči domény, ze všech řadičů udělat globální katalogy (PDC, RID, infrastructure je vhodné mít na jednom řadiči domény)
Není li globální katalog všude pak infrastructure musí jit jinam.
Schéma master a Domain naming se ponechávají spolu v kořenové doméně lesa.
Seize provádět jen v případě ze je to fakt nutné – bez mnoha roli se dá chvíli obejít.

Záloha a obnova active directory

Provádí se NtBackup zaškrtnout položku system state.
Při obnově tímtéž nástrojem **2 možnosti**:

1. **autoritativní obnova** – po dokončení NtBackup obnovy nerestartovat a přes ntdsutil udělat autoritativní obnovu – všecky objekty se nastaví na novější značku a replikuji se do ostatních řadičů
2. **neautoritativní obnova** – po dokončení restartovat, nereplikuji se změny od doby zálohy