Active Directory – část 2

[Povinné]

Operační servery

[Povinné]

V **Active Directory** doméně jsou si všechny řadiče domény rovny. Všechny mohou zapisovat do databáze a replikovat změny ostatním řadičům domény. Ovšem v každé replikační topologii typu *multimaster*[1] existují určité operace, jenž musí být vykonány právě jedním členem (serverem). Členové (servery) jenž v **Active Directory** doméně plní nějakou takovouto specifickou roli se označují jako operační servery (*operations masters*). Ostatní servery jsou samozřejmě také schopny plnit tyto role, ovšem v jednu dobu smí danou roli plnit pouze jediný server. Role se také dělí do dvou kategorií.

Do první kategorie patří role plněné v rámci celého lesa (tzv. *forest-wide* role):

- **Jmenování domén** (*Domain Naming*). Role jmenování domén se používá při přidávání a také odebírání domén v lese. Pokud při vytváření nebo rušení domény není server plnící tuto roli k dispozici, operace selže.
- **Schéma** (*Schema*). Server plnící tuto roli je odpovědný za modifikace schématu daného lesa. Ostatní řadiče domény obsahují pouze *read-only* kopii schématu. Pokud je vyžadována modifikace schématu na serveru, jenž neplní tuto roli, je tento požadavek přeposlán serveru, jenž zastává tuto roli, aby požadované změny provedl. Pokud tento server není k dispozici, modifikaci nepůjde provést.

Druhá kategorie zahrnuje role plněné v rámci konkrétní domény (tzv. *domain-wide*):

- **RID** (*Relative Identifier*). Server plnící tuto roli hraje významnou úlohu při generování **SID** pro bezpečnostní objekty, jako jsou uživatelé, skupiny nebo počítače. **SID** musí být unikátní. Jelikož kterýkoliv řadič domény může vytvářet účty (a tedy i **SID**), musí existovat mechanismus, jenž zajistí unikátnost vytvářených **SID**. Řadiče domény generují **SID** tak, že připojí unikátní **RID** k **SID** domény. **RID** server pro danou doménu přiřazuje rozsah unikátních **RID** každému řadiči domény v dané doméně, takto tedy nemůže dojít k situaci, že dva řadiče domény vytvoří stejné **SID**.
- **Infrastruktura** (*Infrastructure*). V multidoménovém prostředí je obvyklé, že se nějaký objekt odkazuje na objekt patřící do jiné domény. Reference mezi objekty jsou vyjádřeny pomocí tzv. *distinguished names* (DN) jenž identifikují cílový objekt. Pokud je tento cílový objekt přejmenován nebo přesunut, server plnící tuto roli zajistí aktualizaci všech referencí na daný objekt.
- **PDC emulátor** (*PDC Emulator*). Server plnící tuto roli zajišťuje hned několik důležitých funkcí pro danou doménu:
  - **Emuluje funkci PDC** (*Primary Domain Controller*). Ve starých Windows NT 4.0 doménách mohl pouze **PDC** provádět změny v adresáři. Starší aplikace, nástroje a klienti si nejsou vědomi, že nyní může provádět změny v adresáři jakýkoliv řadič domény a vyžadují spojení s **PDC**. **PDC** emulátor zajišťuje zpětnou kompatibilitu **Active Directory** s těmito aplikacemi.
  - **Podílí se na speciální aktualizaci hesel v doméně**. Když je heslo uživatele změněno nebo *resetováno*, dojde okamžitě k replikaci těchto změn na **PDC** emulátor. Pokud uživatel zadá špatné heslo při přihlašování do domény, nedojde ihned k jeho zamítnutí, ale řadič domény, jenž uživatele *autentizuje*, přepošle požadavek na přihlášení **PDC** emulátoru. **PDC** emulátor ověří heslo, a pokud je v pořádku, instruuje řadič domény, aby *autentizaci* povolil. Tato funkce zajistí, že je uživatel autentizován i v případě, že si zrovna změnil heslo a tato změna ještě nebyla replikována na ostatní řadiče domény.

[1] Replikace typu *multimaster* znamená, že replikaci může iniciovat jakýkoliv člen (server), což je umožněno existencí více tzv. *master* kopií replikovaných dat (v případě **Active Directory** má každý řadič domény *master* kopii databáze)

- **Spravuje aktualizace zásad skupiny v doméně**. Při modifikaci zásad skupiny na dvou řadičích domény současně může dojít ke konfliktům při replikaci provedených změn. Aby se vyhnulo těmto situacím, slouží **PDC** emulátor jako ústřední bod pro veškeré změny zásad skupiny. Tedy modifikace zásad skupiny se vždy provádí na **PDC** emulátoru.
- **Poskytuje hlavní zdroj času pro doménu**. Správná synchronizace času jednotlivých systémů je nezbytná pro správné fungování **Active Directory**, Kerberos, FRS, DFS-R apod., jelikož všechny tyto systémy a služby jsou závislé na časových razítkách (*timestamps*). **PDC** emulátor v kořenové doméně lesa je hlavní zdroj času pro celý les. **PDC** emulátory v každé doméně se synchronizují s **PDC** emulátorem v kořenové doméně lesa. Ostatní řadiče domény se pak synchronizují s **PDC** emulátorem v jejich doméně. Všechny ostatní počítače se nakonec synchronizují s některým z řadičů domény. Tento hierarchický přístup zajišťuje konzistenci času a je realizován službou Win32Time.
- **Působí jako doménový prohlížeč** (*domain master browser*). Při procházení sítě se klientovi zobrazují okolní domény a počítače ve formě tzv. *browse listu*. Tyto *browse listy* jsou vytvářeny službou prohlížeče (*browser*) na každém segmentu sítě. Doménový prohlížeč slučuje tyto *browse listy* do jediného, jenž je pak poskytnut klientům.

Globální katalog

[Povinné]

Globální katalog je speciální oddíl, jenž uchovává informace o všech objektech v daném lese. Tyto informace jsou ovšem značně omezené, neuchovávají se informace o všech atributech jednotlivých objektů, ale pouze část těchto atributů, které jsou výhodné z hlediska vyhledávání. Globální katalog se proto často označuje jako tzv. *partial attribute set* (PAS) a lze ho považovat za jakýsi index pro datové úložiště **Active Directory**.

Kterýkoliv řadič domény může obsahovat globální katalog, obecně se doporučuje mít alespoň dva řadiče domény s globálním katalogem v každé doméně. Globální katalogy výrazně zvyšují efektivitu adresářových služeb, ideálně lze mít globální katalog na každém řadiči domény. Více globálních katalogů na druhou stranu znamená také větší objem dat pro replikaci, což ovšem dnes nebývá problém. Globální katalogy také obsahují informace o univerzálních skupinách.

Studentské 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 S00 – konfigurace virtuálních stanic

[Projít]

Připojte sítové adaptéry stanic k následujícím virtuálním přepínačům:

Adaptér (MAC suffix)	LAN1 (-01)	LAN2 (-02)	LAN3 (-03)	LAN4 (-04)
w10-domain	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno
D+R+C w2016-dc	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno
D+R+C w2016-repl	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

Lab X01 – ADAC (Active Directory Administrative Center)

[Projít]

Cíl cvičení

Seznámit se s administrativním centrem AD

Potřebné virtuální stroje

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

Otevřete administrativní centrum **Active Directory** (např. z nabídky Tools v server manageru). Prozkoumejte hierarchii kontejnerů.

Vytvořte organizační jednotku **brno** přímo pod doménou **testing.local** a uživatele **marge** v kontejneru Users.

Otevřete vlastnosti uživatele **marge** a prozkoumejte nastavení. ADAC je nový nástroj a novější funkcionalita, např. *zásady hesel* (fine-grained password policies), ovládání *active directory koše* a nastavení *dynamického řízení přístupu*, zde lze nastavit mnohem pohodlněji. Najděte jak uživateli resetovat heslo a odblokovat účet přímo na úvodní stránce/dashboardu.

Lab X02 – Operační servery (Operations Masters) a globální katalog [Projít]

Cíl cvičení

Seznámit se s operačními servery.

Potřebné virtuální stroje

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

Prozkoumejte, kde lze nastavit jednotlivé operační servery:

- **RID**, **PDC** a **Infrastructure** v **Active Directory Users and Computers** (pravý klik na **testing.local** → Operations Masters…).
- **Domain Naming** v **Active Directory Domains and Trusts** (Action → Operations Master…).
- **Schema** v **Active Directory Schema** (zaregistrovat příkazem **regsvr32 schmmgmt.dll** MMC snap-in, v něm Action pak→ Operations Master…).

Podívejte se, kde se nastavuje přítomnost globálního katalogu na řadiči v **Active Directory Sites and Services** (Sites → Default-First-Site-Name → Servers → w2016-dc, pravý klik na NTDS Settings, vybrat Properties, záložka General).

Lab S01 – Správa Active Directory pomocí Windows PowerShell (s modulem ActiveDirectory) [Povinné]

Cíl cvičení

Seznámit se se základními příkazy **Windows PowerShell** pro vytváření, modifikaci a mazání objektů **Active Directory** z modulu ActiveDirectory (lze použít na Windows Serveru 2012 a novějších).

Potřebné virtuální stroje

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

Další prerekvizity

Organizační jednotka **brno** pod **testing.local**

1. Na **w2016-dc** se přihlaste jako uživatel **administrator** do domény **testing.local**
2. Spusťte **Windows PowerShell**
   - Pro následující příkazy (cmdlety) je potřeba modul ActiveDirectory. Jeho import probíhá v PowerShellu od verze 3.0 (obsaženém od Windows Serveru 2012) automaticky při prvním použití některého z obsažených příkazů. Pokud tomu tak nebude, použijte příkaz **import-module ActiveDirectory**. Alternativně lze použít zástupce **Active Directory Module for Windows Powershell** z **Administrative Tools**
3. Přidejte nového uživatele **lisa** do organizační jednotky **brno**
   a. Spusťte příkaz **New-ADuser lisa -Path "OU=brno,DC=testing,DC=local"**
   b. Ověřte v **Active Directory Users and Computers**, že uživatel byl přidán
      - Protože jsme nedefinovali heslo, bude účet zakázán
      - Pokud uživatele v zadané OU nevidíte, zkuste použít refresh

4. Změňte uživateli **lisa** heslo
   a. Spusťte příkaz **Set-ADAccountPassword "CN=lisa,OU=brno,DC=testing,DC=local" -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "aaa" -Force)**
      - Místo DN lze použít i jen **-Identity lisa** (viz následující bod)
5. Povolte účet uživatele **lisa** a zařiďte, aby **lisa** nemusela měnit heslo při prvním přihlášení
   a. Spusťte příkaz **Set-ADUser -Identity lisa -ChangePasswordAtLogon $false –Enabled $true**
   b. Ověřte změnu v **Active Directory Users and Computers**
      - Volitelně: Ověřte funkčnost vytvořeného účtu přihlášením do domény **testing.local** na **w10-domain** jako uživatel **lisa**
6. Nastavte uživateli **lisa** příjmení (pomocí **Set-ADUser**)
   - samostatně, pokud si nevíte rady, zeptejte se lektora
7. Vypište informace o uživateli lisa
   a. Spusťte příkaz **Get-ADUser -identity lisa**
8. Vytvořte organizační jednotku **vut** pod organizační jednotkou **brno**
   a. Spusťte příkaz **New-ADOrganizationalUnit vut -Path "OU=brno,DC=testing,DC=local"**
   b. Ověřte v **Active Directory Users and Computers**, že organizační jednotka byla vytvořena
9. Přesuňte uživatele **lisa** do organizační jednotky **vut**
   a. Spusťte příkaz **Move-ADObject "CN=lisa,OU=brno,DC=testing,DC=local" -TargetPath "OU=vut,OU=brno,DC=testing,DC=local"**
   b. Ověřte přesun v **Active Directory Users and Computers**
10. Ověřte přesunutí vypsáním všech uživatelů v organizační jednotce **vut**
    a. Spusťte příkaz **Get-ADUser -Filter * -SearchBase "OU=vut, OU=brno, DC=testing, DC=local" | select name, surname, enabled**
11. Zobrazte jméno, příjmení a stav pro všechny zakázané uživatelské účty v Objektu Users
    a. Spusťte příkaz **Get-ADUser -Filter * -SearchBase "CN=users, DC=testing, DC=local" | where {$_.enabled –eq $false} | select name, surname, enabled**
12. Smažte organizační jednotku **vut** i s celým jejím obsahem (bez potvrzování)
    a. Spusťte příkaz **Remove-ADOrganizationalUnit -Identity "OU=vut, OU=brno, DC=testing, DC=local" -Recursive -confirm:$false**
       - Nemělo by se podařit
    b. Zrušte ochranu proti náhodnému smazání pomocí příkazu **Set-ADOrganizationalUnit -Identity "OU=vut, OU=brno, DC=testing, DC=local" -ProtectedFromAccidentalDeletion $false**
    c. Pokuste se znova o smazání
    d. Ověřte v **Active Directory Users and Computers**, že organizační jednotka byla smazána

Lab S02 – Správa Active Directory pomocí Windows PowerShell pomocí pokročilých metod [Volitelné]

Cíl cvičení

Seznámit se se základními příkazy **Windows PowerShell** pro vytváření, modifikaci a mazání objektů **Active Directory** bez použití modulu ActiveDirectory (lze použít na Windows Serveru 2008 a novějších).

Potřebné virtuální stroje

w2016-dc (D+R+C w2016-dc)
w10-domain

Další prerekvizity

Organizační jednotka **brno** pod **testing.local**

13. Na **w2016-dc** se přihlaste jako uživatel **administrator** do domény **testing.local**
14. Spusťte **Windows PowerShell**
15. Přidejte nového uživatele **lisa** do organizační jednotky **brno**
    a. Získejte referenci na objekt, jenž reprezentuje organizační jednotku **brno** pomocí příkazu **$ouBrno = [ADSI]"LDAP://OU=brno,DC=testing,DC=local"**
    b. Vytvořte uživatele **lisa** příkazem **$userLisa = $ouBrno.Create("user", "CN=lisa")**
    c. Potvrďte vytvoření uživatele příkazem **$userLisa.SetInfo()**
    d. Ověřte v **Active Directory Users and Computers**, že uživatel byl přidán
16. Změňte uživateli **lisa** heslo
    a. Získejte referenci na objekt, jenž reprezentuje uživatele **lisa** pomocí příkazu **$userLisa = [ADSI]"LDAP://CN=lisa,OU=brno,DC=testing,DC=local"**
    b. Změňte heslo uživatele **lisa** příkazem **$userLisa.SetPassword("aaa")**
    c. Potvrďte změnu hesla příkazem **$userLisa.SetInfo()**
17. Povolte účet uživatele **lisa**
    a. Získejte referenci na objekt, jenž reprezentuje uživatele **lisa** pomocí příkazu **$userLisa = [ADSI]"LDAP://CN=lisa,OU=brno,DC=testing,DC=local"**
    b. Povolte účet příkazem **$userLisa.InvokeSet("AccountDisabled", $false)**
    c. Potvrďte povolení účtu příkazem **$userLisa.SetInfo()**
        - Volitelně: Ověřte funkčnost vytvořeného účtu přihlášením do domény **testing.local** na **w10-domain** jako uživatel **lisa**
18. Vytvořte organizační jednotku **vut** pod organizační jednotkou **brno**
    a. Získejte referenci na objekt, jenž reprezentuje organizační jednotku **brno** pomocí příkazu **$ouBrno = [ADSI]"LDAP://OU=brno,DC=testing,DC=local"**
    b. Vytvořte organizační jednotku **vut** pod organizační jednotkou **brno** příkazem **$ouVut = $ouBrno.Create("organizationalUnit", "OU=vut")**
    c. Potvrďte vytvoření organizační jednotky příkazem **$ouVut.SetInfo()**
    d. Ověřte v **Active Directory Users and Computers**, že organizační jednotka byla vytvořena
19. Přesuňte uživatele **lisa** do organizační jednotky **vut**
    a. Získejte referenci na objekt, jenž reprezentuje uživatele **lisa** pomocí příkazu **$userLisa = [ADSI]"LDAP://CN=lisa,OU=brno,DC=testing,DC=local"**
    b. Získejte referenci na objekt, jenž reprezentuje organizační jednotku **vut** pomocí příkazu **$ouVut = [ADSI]"LDAP://OU=vut,OU=brno,DC=testing,DC=local"**

   c. Přesuňte uživatele **lisa** do organizační jednotky **vut** příkazem **$userLisa.MoveTo($ouVut, "CN=lisa")**
20. Ověřte přesunutí vypsáním všech uživatelů v organizační jednotce **vut**
   a. Získejte referenci na objekt, jenž reprezentuje organizační jednotku **vut** pomocí příkazu **$ouVut = [ADSI]"LDAP://OU=vut,OU=brno,DC=testing,DC=local"**
   b. Vypište seznam všech uživatelů v organizační jednotce **vut** příkazem **$ouVut.Children | Format-List -property distinguishedName**
21. Změňte uživateli **lisa** příjmení
   a. Získejte referenci na objekt, jenž reprezentuje uživatele **lisa** pomocí příkazu **$userLisa = [ADSI]"LDAP://CN=lisa,OU=vut,OU=brno,DC=testing,DC=local"**
   b. Změňte příjmení uživatele **lisa** příkazem **$userLisa.put("sn", "Simpson")**
   c. Potvrďte změnu příjmení příkazem **$userLisa.SetInfo()**
22. Ověřte změnu příjmení
   a. Získejte referenci na objekt, jenž reprezentuje uživatele **lisa** pomocí příkazu **$userLisa = [ADSI]"LDAP://CN=lisa,OU=vut,OU=brno,DC=testing,DC=local"**
   b. Vypište přehledně informace o uživateli **lisa** příkazem **$userLisa | Format-List ***
   c. Vypište pouze informace o příjmení příkazem **$userLisa | Format-List -property sn**
23. Smažte organizační jednotku **vut** i s celým jejím obsahem
   a. Získejte referenci na objekt, jenž reprezentuje organizační jednotku **vut** pomocí příkazu **$ouVut = [ADSI]"LDAP://OU=vut,OU=brno,DC=testing,DC=local"**
   b. Smažte organizační jednotku **vut** příkazem **$ouVut.DeleteTree()**
24. Ověřte v **Active Directory Users and Computers**, že organizační jednotka byla smazána

Lab S03 – Přesun operačního serveru (Operations Master) [Povinné]

Cíl cvičení

Přesunout PDC emulátor na jiný řadič domény

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 **Active Directory Users and Computers**
   a. Start → Administrative Tools → Active Directory Users and Computers
3. Připojte se na **w2016-repl**
   a. Klikněte pravým na **testing.local** a zvolte Change Domain Controller…
   b. V Change Directory Server zvolte This Domain Controller or AD LDS instance a v seznamu vyberte **w2016-repl.testing.local**
   c. Potvrďte OK
4. Přesuňte roli **PDC** emulátoru na **w2016-repl**
   a. Klikněte pravým na **testing.local** a zvolte Operations Masters…
   b. Přejděte na záložku PDC
   c. Zvolte Change…
   d. Přesuňte roli pomocí Yes
   e. Potvrďte přesunutí role pomocí OK