

## RODC (Read-Only Domain Controller)

[ Povinné ]

Pokud je nějaká doména rozprostřena přes více míst (*sites*), nastává otázka, kde umístit jednotlivé řadiče domény. Síťová propojení mezi místy nejčastěji vytvářejí hvězdicovou topologii, existuje tedy jedno hlavní místo (*hub site, main office*), jenž je spojeno se všemi ostatními vedlejšími místy (*branch office*). Obecně lze říci, že vedlejší místa nikdy nedosahují takové úrovně zabezpečení, jakou má místo hlavní. Spojení mezi hlavním a vedlejším místem bývá pomalé, což vede často k jeho zahlcení, nebo nespolehlivé, kdy může docházet k častým výpadkům. Nakonec, vedlejší místa mívají velice omezený personál pro správu řadičů domény a techniky obecně.

Asi nejlepším řešením by bylo umístit všechny řadiče domény do hlavního místa. Tento postup ale vede k několika problémům:

- **Autentizace.** Zde je dobré rozlišovat dva typy *autentizace* – do domény a ke službám. V obou případech musí *autentizaci* provést řadič domény, jenž se nachází v hlavním místě. Tedy tato *autentizace* probíhá přes (potenciálně pomalé) spojení mezi vedlejším a hlavním místem. Pokud je toto spojení přerušeno, nemůže se uživatel přihlásit. Jelikož se ale uživatel přihlašuje většinou jen jednou denně, není tento typ *autentizace* až tak kritický. V případě *autentizace* ke službám se využívá tzv. *service tickets*, jakýchsi klíčů, jenž umožňují uživateli přistupovat ke specifickým službám. Tyto klíče vydávají řadiče domény jednotlivým uživatelům. Protože uživatel často využívá více služeb během jednoho dne, je pro tento typ *autentizace* nezbytné mít rychlé a spolehlivé spojení s řadičem domény v hlavním místě.
- **Vyhledávání.** K vyhledávání informací v doméně je potřeba globální katalog. Všechny dotazy musí být tedy přeposílány řadičům domény v hlavním místě, které nesou globální katalog. To vede k dalšímu zahlcování spojení a pomalému vyhledávání.

Nasazení řadičů domény do vedlejších míst sice vyřeší výše zmíněné problémy, ale za cenu vytvoření problémů nových:

- **Správa.** V případě údržby řadiče domény (např. instalace ovladače pro nový hardware) je potřeba se na něj přihlásit jako lokální správce (člen skupiny *Administrators*). Ovšem na řadičích domény jsou všichni lokální správci zároveň také správci domény (členové *Domain Admins*) a mohou tedy spravovat celou doménu. Většinou není vhodné, aby lokální správci ve vedlejším místě měli takovéto možnosti, jelikož to zvyšuje nebezpečí výskytu problémů popsaných níže.
- **Konzistence.** Veškeré změny v **Active Directory** databázi na řadiči domény ve vedlejším místě jsou replikovány na ostatní řadiče domény. Poškození databáze může vážně narušit integritu doménových služeb, jelikož chybná data mohou být replikována do celé domény.
- **Bezpečnost.** Každý řadič domény uchovává kopii veškerých informací o všech objektech v doméně, včetně tajných informací jako uživatelských hesel. V případě nepovoleného přístupu či odcizení řadiče domény je možné tyto informace získat.

**RODC** řadiče jsou speciální řadiče domény určené primárně pro nasazení do vedlejších míst. Každý **RODC** řadič obsahuje kopii veškerých objektů domény a jejich atributů, stejně jako každý normální řadič domény, s výjimkou atributů obsahujících tajné informace, jako jsou hesla. **RODC** řadič tedy nemůže provádět *autentizaci*. Lze ale nastavit zásadu replikace hesel (PRP, *Password Replication Policy*), která umožňuje specifikovat uživatele, jejichž účty bude **RODC** řadič uchovávat ve své vyrovnávací paměti (*kešovat*). Pokud se takovýto uživatel přihlásí, uloží **RODC** řadič jeho pověření<sup>1</sup> (*credentials*) do své vyrovnávací paměti. Při příštím přihlašování tohoto uživatele použije **RODC** řadič informace uložené v této paměti namísto toho, aby žádost o přihlášení přeposlal k vyřízení normálnímu řadiči domény. Navíc si normální řadiče domény uchovávají informace o tom, která pověření jsou přítomna ve vyrovnávacích pamětech jednotlivých **RODC** řadičů. V případě, že dojde k odcizení

<sup>1</sup> Pověření je sada informací sloužící k *autentizaci* určité entity (uživatele, počítače apod.), v případě uživatele to jsou nejčastěji informace o uživatelském jméně a hesle

nějakého **RODC** řadiče a je potřeba nastavit nová hesla pro uživatele, jejichž účty byly *kešované*, jsou tyto informace k dispozici. Přesněji, při odstranění účtu **RODC** řadiče z **Active Directory** systém automaticky nabídne možnost provést *reset* uživatelských hesel pro *kešované* účty.

Kopie **Active Directory** databáze, kterou obsahují **RODC** řadiče je určena pouze pro čtení, nelze do ní tedy přímo zapisovat. Pokud nějaká aplikace potřebuje číst z **Active Directory**, zpracuje **RODC** řadič tento požadavek a povolí jí přístup. V případě zápisu je aplikace přesměrována na normální řadič domény, který provede požadované změny v **Active Directory** databázi. Tyto změny jsou pak replikovány na ostatní řadiče domény, včetně **RODC** řadičů. Replikace je z pohledu **RODC** řadičů jednosměrná, probíhá vždy pouze z normálních řadičů domény na **RODC** řadiče, nikdy opačně. To zabraňuje situaci, že dojde k replikaci podvržených či poškozených dat v **Active Directory** databázi a také redukuje zátěž tzv. *bridgehead* serverů (viz pozdější sekce). Jednosměrná replikace se týká také adresáře **SYSVOL**. Do tohoto adresáře mohou sice **RODC** řadiče zapisovat, ale stejně jako v případě **Active Directory** databáze nebudou tyto změny replikovány na ostatní řadiče domény.

U **RODC** řadičů může být funkce lokálního administrátora delegována jakémukoliv doménovému uživateli nebo bezpečnostní skupině (*security group*). Takto pověření uživatelé se mohou přihlásit na daný **RODC** řadič a provádět akce spojené s údržbou, aniž by zároveň získali nadměrná oprávnění pro akce v rámci domény. Tito uživatelé se také nemohou přihlásit na žádný jiný řadič domény.

**RODC** řadiče mohou samozřejmě plnit úlohu **DNS** serveru. V případě, že je spravovaná zóna integrována do databáze **Active Directory** jsou zde ale rozdíly. Stejně jako celá databáze **Active Directory** i v ní integrované zóny jsou určeny pouze pro čtení. Tyto zóny lze považovat za obdobu sekundárních zón u systému **DNS**. Jediná možnost jak změnit obsah takovéto zóny je skrz replikaci. Díky tomu také **RODC** řadiče nepodporují dynamické aktualizace **DNS** záznamů klienty, které musí probíhat nepřímo. Pokud se klient pokusí aktualizovat svůj **DNS** záznam u **RODC** řadiče, vrátí mu řadič odkaz na jiný **DNS** server. Klient pak zkusí aktualizovat svůj záznam u tohoto **DNS** serveru. Zároveň se **RODC** řadič pokusí replikovat klientem aktualizovaný záznam z tohoto **DNS** serveru. Tato replikace je ovšem speciální, týká se pouze jediného objektu, pouze aktualizovaného záznamu. Ostatní změny nejsou replikovány.

I přesto, že **RODC** řadiče mohou plnit různé role, nemohou být nikdy operačními servery. Mohou ovšem nést globální katalog, což je důležité pro vyhledávání.

## Instalace

[ Povinné ]

Než je možné povýšit nějaký server do role **RODC** řadiče, je nejprve potřeba ověřit splnění několika podmínek a případně připravit daný les na nasazení **RODC** řadičů. Proces instalace **RODC** řadičů se dá rozdělit na tři části:

- **Ověření požadavků.** Nasazení **RODC** řadičů vyžaduje, aby funkční úroveň lesa byla minimálně [Windows Server 2003](#). Je tedy potřeba ověřit, že na všech řadičích domény v daném lese běží systém Windows Server 2003. Pak zkontrolovat funkční úroveň všech domén v daném lese a případně ji zvýšit na úroveň [Windows Server 2003](#). Potom už jen zbývá ověřit funkční úroveň samotného lesa. Druhým požadavkem je existence minimálně jednoho normálního řadiče domény v dané doméně, na němž běží alespoň Windows Server 2008. **RODC** řadiče totiž mohou replikovat doménová data<sup>2</sup> jen z takovýchto řadičů domény, nelze je nikdy replikovat z jiných **RODC** řadičů ani z normálních řadičů domény, na nichž běží Windows Server 2003 nebo starší systém. Pokud **RODC** řadič plní i úlohu **DNS** serveru, musí nějaký z řadičů domény, na kterých běží Windows Server 2008 a novější, také obsahovat danou **DNS** zónu.
- **Příprava lesa.** Protože **RODC** řadiče mohou být nainstalovány jen na počítače, na kterých běží Windows Server 2008 nebo novější, musí být možné přidat počítače s tímto systémem do existujícího lesa. V případě existujícího lesa (s funkční úrovní [Windows Server 2003](#) a nižší), je

<sup>2</sup> Doménovými daty rozumíme veškerá data, jež podléhají replikaci z hlediska **Active Directory**, nejsou to tedy jen data z databáze **Active Directory**, ale např. i data z adresáře **SYSVOL** apod.

nutné připravit tento les pomocí **adprep /forestprep** a následně umožnit existenci **RODC** řadičů v doménách pomocí **adprep /rodcprep**. Tyto příkazy slouží k aktualizaci schématu daného lesa.

- **Instalace.** Do role **RODC** řadiče lze povýšit jakýkoliv počítač, na kterém běží Windows Server 2008 nebo novější. Instalace se provádí stejně jako u normálních řadičů domény. (I Windows **Server 2008 Core** může plnit úlohu **RODC** řadiče, je však potřeba provést bezobslužnou instalaci). Je také možné delegovat instalaci **RODC** řadiče na uživatele, jenž není správce domény. Stačí předpřipravit účet pro instalovaný **RODC** řadič v organizační jednotce Řadiče domény (*Domain Controllers*) a specifikovat účet, jenž bude použit pro připojení tohoto řadiče do domény. Server, který bude povýšen do role **RODC** řadiče, musí být člen pracovní skupiny. Pokud by byl v doméně, nebude se moci navázat na předpřipravený účet.

## Fine-Grained zásady hesel a uzamykání účtů

[ Povinné ]

Zásady hesel (*Password Policies*) a zásady uzamykání účtů (*Account Lockout Policies*) se nacházejí pod uzlem nastavení počítače (*Computer Configuration*). Tyto zásady jsou tedy vždy aplikovány pouze na počítače, ne na uživatele. Výjimkou jsou nastavení obsažená v **GPO** objektu [Default Domain Policy](#), která jsou aplikována na veškeré uživatele v dané doméně. Pokud bylo dříve potřeba změnit nastavení těchto zásad pouze pro některé uživatele, nebylo to jednoduše možné. Jedinou možností bylo použití speciálních filtrů pro hesla nebo nasazení více domén s odlišným nastavením [Default Domain Policy](#)<sup>3</sup>. Od systému Windows Server 2008 lze tento problém řešit pomocí tzv. *fine-grained* zásad hesel.

**Fine-grained zásady hesel** (*fine-grained password and lockout policies*, či jen *fine-grained policies*) umožňují definovat zásady hesel a uzamykání účtů pro jednotlivé skupiny nebo uživatele v doméně. Aby bylo možné používat tyto zásady v dané doméně, musí být její funkční úroveň alespoň [Windows Server 2008](#).

## Objekty nastavení hesel

[ Povinné ]

Zásady spravované *fine-grained* zásadami hesel jsou totožné se zásadami pod uzly Zásady hesla (*Password Policy*) a Zásady uzamčení účtů (*Account Lockout Policy*) v **GPO** objektech. *Fine-grained* zásady hesel ale nejsou implementovány jako součást zásad skupiny, ani nejsou aplikovány jako **GPO** objekty. Jsou uloženy ve speciálním objektu **Active Directory** označovaném Objekt nastavení hesel (**PSO**, *Password Settings Object*). V doméně může existovat neomezené množství **PSO** objektů. **PSO** objekt může být připojen (*linked*) k jedné či více globálním bezpečnostním skupinám (*global security group*) nebo uživatelům. K jiným typům skupin nelze připojit.

Stejně jako u **GPO** objektů, i u **PSO** objektů může být jeden **PSO** objekt přiřazen k více skupinám či uživatelům. Navíc jeden uživatel může být členem hned několika skupin. Na rozdíl od **GPO** objektů ale **PSO** objekty vždy definují veškeré obsažené zásady, tedy vždy pouze jediný **PSO** objekt určuje výsledná nastavení aplikovaná na daného uživatele. Každý **PSO** objekt obsahuje atribut, který určuje jeho prioritu. Priorita je, stejně jako u **GPO** objektů, nezáporné číslo, kdy menší číslo znamená vyšší prioritu. Pokud je na uživatele aplikováno více **PSO** objektů, projeví se nastavení z toho, jenž má nejvyšší prioritu. Pravidla pro určení výsledné priority jsou následující:

- Pokud je ke skupinám, jejichž členem je daný uživatel, připojeno více **PSO** objektů, vybere se ten s nejvyšší prioritou.
- Pokud je jeden nebo více **PSO** objektů připojeno přímo k danému uživateli, jsou **PSO** objekty připojené ke skupinám ignorovány, nezávisle na jejich prioritě. Ze všech **PSO** objektů připojených k danému uživateli se vybere ten s nejvyšší prioritou.

<sup>3</sup> Existuje ještě možnost přepsat některá nastavení u jednotlivých uživatelských účtů (na záložce nastavení účtu ve vlastnostech uživatele), ovšem většina důležitých nastavení tam chybí a také není únosné nastavovat vše pro každého uživatele zvlášť

- Pokud má více **PSO** objektů stejnou prioritu, vybere **Active Directory** ten, jenž má nejnížší hodnotu **GUID** identifikátoru. Jelikož žádné dva objekty v **Active Directory** nemají stejný **GUID** identifikátor, je zajištěno, že takto musí být vybrán pouze jediný **PSO** objekt. Je pouze na uživateli, aby nastavil priority **PSO** objektů tak, aby k této situaci nemohlo dojít.

**Active Directory** ukládá u každého uživatele informaci o výsledném **PSO** objektu, jenž bude na tohoto uživatele aplikován. Tato informace je uložena ve formě atributu objektu uživatele.

Je důležité si uvědomit, že **PSO** objekty jsou připojovány pouze ke skupinám a uživatelům. Nelze je připojit k organizačním jednotkám, jak tomu je v případě **GPO** objektů. Jedinou možností jak aplikovat nastavení v **PSO** objektu na uživatele v nějaké organizační jednotce je vytvořit novou skupinu, do které se zařadí všichni uživatelé z dané organizační jednotky. Tyto skupiny se často označují jako tzv. stínové skupiny (*shadow groups*).

## Společné 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 LS00 – konfigurace virtuálních stanic

[\[ Provést \]](#)

Připojte síťové adaptéry stanic k následujícím virtuálním přepínačům:

Adaptér (MAC suffix)	LAN1 (-01)	LAN2 (-02)	LAN3 (-03)	LAN4 (-04)
<b>D+R+C w2016-dc</b>	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno
<b>D+R+C w2016-repl</b>	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno
<b>w2016-base</b>	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.
- Na stanici **D+R+C w2016-dc** restartujte službu DHCP
  - DHCP MMC, vyberte w2016-dc.testing.local a z kontextové nabídky All Tasks – Restart
- Tip: stanice **D+R+C w2016-dc** a **D+R+C w2016-repl** spusťte na začátku cvičení.

## Lektorské úkoly

### Lab L01 – Instalace RODC

[ Provést ]

#### Cíl cvičení

Přidat RODC řadič do existující domény

#### Potřebné virtuální stroje

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

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

**w2016-base**

#### Další prerekvizity

- globální bezpečnostní skupina (*global security group*) **Simpsons** v doméně **testing.local**
- účet uživatele **student** v doméně **testing.local**, který není členem skupiny **Simpsons**
- účet uživatele **homer** v doméně **testing.local**, jenž je členem skupiny **Simpsons**

1. Na **w2016-base** se přihlaste jako lokální uživatel **administrator**
2. Nastavte statickou IPv4 adresu **192.168.32.9** jako IPv4 adresu počítače a IPv4 adresu **192.168.32.5** jako IPv4 adresu DNS serveru
  - a. Otevřete **Network and Sharing Center**, zvolte **LAN2** a pak **Properties**
    - Zvolené síťové rozhraní musí odpovídat **Private1**, standardně to je **LAN2**
  - b. Vyberte **Internet Protocol Version 4 (TCP/IPv4)** a zvolte **Properties**
  - c. Zvolte **Use the following IP address** a jako IP address zadejte **192.168.32.9**
  - d. Klikněte do zadávacího pole u **Subnet mask**, maska podsítě bude doplněna automaticky
  - e. Pod **Use the following DNS server addresses** zadejte **192.168.32.5** do pole **Preferred DNS Server**
  - f. Potvrďte **OK** a dvakrát **Close**
3. Nainstalujte roli **Active Directory Domain Services**
  - a. Spusťte **Server Manager**
    1. **Start** → **Server Manager**
  - b. Vyberte **Add Roles and Features** z nabídky **Manage**
  - c. Pokračujte **Next >**
  - d. Vyberte **Role-based or feature-based installation** a pokračujte **Next >**
  - e. Vyberte aktuální server a pokračujte **Next >**
  - f. V seznamu rolí vyberte **Active Directory Domain Services**, potvrďte přidání potřebných funkcí **Add Features** a pokračujte třikrát **Next >**
  - g. Potvrďte instalaci **Install**
  - h. Po dokončení instalace najdete v notifikacích **Server Manageru** odkaz na **Promote this server to a domain controller**
4. V konfiguračním průvodci (**Active Directory Domain Services Configuration Wizard**)
  - a. V kroku **Deployment Configuration**
    1. Zvolte **Add a domain controller to an existing domain**
    2. Do pole **Domain** zadejte **testing.local**
    3. Klepněte na tlačítko **Change...** v sekci **Supply the credentials to perform this operation** a vyplňte jméno **testing\administrator** a heslo **aaa**
      - Lze použít i zápis **administrator@testing.local**
    4. Pokračujte **Next >**

- b. V části [Domain Controller Options](#)
    - 1. ponechte zaškrtnuté možnosti **DNS server** i **Global Catalog**
    - 2. zaškrtněte **Read-only Domain Controller (RODC)**.
    - 3. v [Site name](#) ponechte místo **Default-First-Site-Name**
    - 4. Jako [Directory Services Restore Mode \(DSRM\) Password](#) použijte (a potvrďte) heslo **aaa**
    - 5. pokračujte [Next >](#)
  - c. V části [RODC Options](#) zvolte skupinu **Simpsons** jako správce instalovaného RODC řadiče
    - 1. Pod [Delegated administrator account](#) použijte [Select...](#)
      - a. V [Enter the object names to select](#) zadejte **Simpsons** a zvolte [Check Names](#) pro ověření existence zadané skupiny
      - b. Potvrďte [OK](#)
    - 2. Zkontrolujte uživatelské skupiny, jejichž hesla se budou/nebudou replikovat na tento RODC
    - 3. Pokračujte [Next >](#)
  - d. V části [Additional Options](#) zvolte, odkud proběhne úvodní replikace
    - 1. Z nabídky [Replicate from](#) zvolte **w2016-dc.testing.local**
    - 2. Pokračujte [Next >](#)
  - e. Zadejte cesty k databázím [Location for Database, Log Files, and SYSVOL](#) (ponechte výchozí). [Next >](#)
  - f. Zkontrolujte zadané údaje a zobrazte si odpovídající **skript pro PowerShell** ([View Script](#)). Pokračujte [Next >](#)
  - g. Prohlédněte si výsledky kontroly prerekvizit.
  - h. Dokončete průvodce [Install](#)
4. Přihlaste se na **w2016-base** jako uživatel **student**
- Přihlášení nebude úspěšné, jelikož standardní uživatel nemá právo přihlašovat se lokálně na řadiče domény (nepatří mezi lokální administrátory)
5. Přihlaste se na **w2016-base** jako uživatel **homer**
- Přihlášení bude úspěšné, jelikož skupina **Simpsons** patří mezi lokální administrátory, kteří jsou na rozdíl od normálních řadičů domény přítomni, u normálních řadičů domény patří mezi lokální administrátory vždy pouze členové **Domain Admins** skupiny bez možnosti to jakkoliv změnit



## Studentské úkoly

### Lab S01 – Zásady replikace hesel

[ Povinné ]

#### Cíl cvičení

Umožnit ukládání hesel vybraných uživatelů ve vyrovnávací paměti RODC řadiče

#### Potřebné virtuální stroje

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

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

**w2016-base**

#### Další prerekvizity

Dokončený úkol **Lab L01**, účty uživatelů **homer** a **bart** v doméně **testing.local**, kteří jsou členy skupiny **Simpsons**

1. Na **w2016-dc** se přihlaste jako uživatel **administrator** do domény **testing.local**
2. Otevřete **ADUC** (*Active Directory Users and Computers*)
  - a. **Start** → **Administrative Tools** → **Active Directory Users and Computers**
3. Povolte pro všechny uživatele ze skupiny **Simpsons** ukládání hesel do vyrovnávací paměti na **w2016-base**
  - a. Vyberte organizační jednotku **Domain Controllers**, klikněte pravým na **w2016-base** a zvolte **Properties**
  - b. Přejděte na záložku **Password Replication Policy** a zvolte **Add...**
  - c. Vyberte **Allow passwords for the account to replicate to this RODC** a pokračujte **OK**
  - d. Do **Enter the object names to select** zadejte **Simpsons** a zvolte **Check Names**
  - e. Potvrďte dvakrát pomocí **OK**
    - V praxi by bylo vhodnější vyrobit speciální skupinu pro daný RODC, které tímto postupem povolíme/zakážeme ukládání hesel, a skupinu **Simpsons** přidat až do této speciální skupiny. V případě povolení/zakázání pro všechny RODC lze využít **Allowed RODC Password Replication Group** a **Denied RODC Password Replication Group**.
4. Přihlaste se na **w2016-base** jako uživatel **homer**
5. Vraťte se zpět na **w2016-dc** do **ADUC**
6. Ověřte, že heslo bylo přihlášením skutečně uloženo ve vyrovnávací paměti **w2016-base**
  - a. Vyberte organizační jednotku **Domain Controllers**, klikněte pravým na **w2016-base** a zvolte **Properties**
  - b. Přejděte na záložku **Password Replication Policy** a zvolte **Advanced...**
  - c. Na záložce **Policy Usage** zvolte **Accounts whose passwords are stored on this Read-only Domain Controller** pod **Display users and computers that meet the following criteria**
  - d. Ověřte, že uživatel **homer** je v seznamu pod **Users and computers**
7. Vložte heslo uživatele **bart** do vyrovnávací paměti **w2016-base**
  - a. Vyberte organizační jednotku **Domain Controllers**, klikněte pravým na **w2016-base** a zvolte **Properties**
  - b. Přejděte na záložku **Password Replication Policy** a zvolte **Advanced...**
  - c. Na záložce **Policy Usage** zvolte **Prepopulate Passwords...**
  - d. Do **Enter the object names to select** zadejte **bart** a zvolte **Check Names**
  - e. Potvrďte pomocí **OK**, **Yes** a **OK**



8. Přerušte spojení mezi **w2016-base** a ostatními řadiči domény
  - a. Na **w2016-dc** a **w2016-repl** zakažte síťové rozhraní **LAN2**
    - Zakázané síťové rozhraní musí odpovídat *Private1*, standardně to je **LAN2**
9. Zkuste se přihlásit na **w2016-base** jako uživatel **administrator**
  - Přihlášení nebude úspěšné, protože heslo uživatele **administrator** není obsaženo ve vyrovnávací paměti **w2016-base**
10. Zkuste se přihlásit na **w2016-base** jako uživatel **bart**
  - Přihlášení bude úspěšné, jelikož heslo uživatele **bart** bylo přidáno do vyrovnávací paměti **w2016-base**
11. obnovte spojení mezi **w2016-base** a ostatními řadiči domény
  - a. Na **w2016-dc** a **w2016-repl** povolte síťové rozhraní **LAN2**
    - Povolené síťové rozhraní musí odpovídat *Private1*, standardně to je **LAN2**

## Lab S02 – Fine-Grained zásady hesel s použitím ADAC

[ Povinné ]

### Cíl cvičení

Nastavit různé zásady hesel pro jednotlivé uživatele (skupiny) s pomocí Active Directory Administrative Center

### Potřebné virtuální stroje

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

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

### Další prerekvizity

Účet uživatele **homer** v doméně **testing.local**, který jsou členy skupiny **Simpsons**

1. Na **w2016-dc** se přihlaste jako uživatel **administrator** do domény **testing.local**
2. Otevřete **ADAC** (*Active Directory Administrative Center*)
  - a. **Start** → **Administrative Tools** → **Active Directory Administrative Center**
3. Přejděte do **testing (local) \ System \ Password Settings Container**
4. Klikněte pravým a zvolte **New \ Password Settings**
  - a. Nastavte
    1. **Name**: **Simpsons PSO**
    2. **Precedence**: **1**
      - Hodnota **Precedence** odpovídá hodnotě atributu **msDS-PasswordSettingsPrecedence**. Jde o obdobu *link order* u GPO, jenž udává prioritu PSO objektu, pokud je více PSO objektů přiřazeno jedné skupině či uživateli.
    3. **Enforce minimum password length**: **3**
    4. Zrušte zaškrtnutí **Enforce password history**
    5. Ponechte **Password must meet complexity requirements**
    6. Zrušte zaškrtnutí **Enforce minimum password age**
    7. **Enforce maximum password age**: **90**
    8. Zaškrtněte **Enforce account lockout policy**
    9. **Number of failed logon attempt allowed**: **5**
    10. **Reset failed logon attempts count after**: **60**
    11. **Account will be locked out – For a duration of (mins)**: **1440**
  - b. V sekci **Directly Applies To** přidejte skupinu **Simpsons**
    1. **Add...**

2. Do [Enter the object names to select](#) zadejte **Simpsons** a zvolte [Check Names](#)
3. Potvrďte pomocí [OK](#)
- c. Pokračujte [OK](#)
5. Zjistěte, jaké zásady hesel se vztahují na uživatele **homer**
  - a. Přejděte do [testing \(local\) \ Users](#)
  - b. Klikněte pravým na uživatele **homer** vyberte [View resultant password settings...](#)
6. Zkuste nastavit uživateli **homer** nové heslo **bbb**
  - a. Přejděte do [testing \(local\) \ Users](#)
  - b. Klikněte pravým na uživatele **homer** vyberte [Reset password...](#)
  - c. Zadejte heslo **bbb**
    - Heslo nepůjde vytvořit, jelikož **Simpsons PSO** vyžaduje silná hesla
7. Smažte **Simpsons PSO**
  - a. Přejděte do [testing \(local\) \ System \ Password Settings Container](#)
  - b. Klikněte pravým na objekt **Simpsons PSO** a z kontextové nabídky vyberte [Properties](#)
  - c. Zrušte zaškrtnutí u **Protect from accidental deletion** a pokračujte [OK](#)
  - d. Z kontextové nabídky **Simpsons PSO** vyberte [Delete](#) a smazání potvrďte [Yes](#)

## Lab S03 – Fine-Grained zásady hesel s pomocí ADSI Edit

[ Volitelné ]

### Cíl cvičení

Nastavit různé zásady hesel pro jednotlivé uživatele s využitím nástroje ADSI Edit (používáno před příchodem Windows 2012)

### Potřebné virtuální stroje

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

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

### Další prerekvizity

Účet uživatele **homer** v doméně **testing.local**, který jsou členy skupiny **Simpsons**

1. Na **w2016-dc** se přihlaste jako uživatel **administrator** do domény **testing.local**
2. Otevřete **ADSI Edit** (*Active Directory Services Interfaces Editor*)
  - a. [Start](#) → [Administrative Tools](#) → [ADSI Edit](#)
3. Připojte se k oddílu domény **testing.local**
  - a. Klikněte pravým na **ADSI Edit** a zvolte [Connect to...](#)
  - b. Do pole [Name](#) zadejte **testing.local** a potvrďte pomocí [OK](#)
4. Vytvořte nový PSO (*Password Settings Object*) objekt **Simpsons PSO**
  - a. Vybírejte postupně uzly [testing.local](#), [DC=testing](#), [DC=local](#), [CN=System](#) a [CN=Password Settings Container](#)
  - b. Klikněte pravým na uzel [CN=Password Settings Container](#), vyberte [New](#) a zvolte [Object...](#)
  - c. Pod [Select a class](#) zvolte třídu **msDS-PasswordSettings** a pokračujte [Next >](#)
  - d. U atributu **cn** zadejte do pole [Value](#) název **Simpsons PSO** a pokračujte [Next >](#)
    - Atribut **cn** obsahuje název PSO objektu
  - e. U atributu **msDS-PasswordSettingsPrecedence** zadejte do pole [Value](#) hodnotu **1** a pokračujte [Next >](#)
    - Atribut **msDS-PasswordSettingsPrecedence** je obdoba *link order* u GPO, jenž udává prioritu PSO objektu, pokud je více PSO objektů přiřazeno jedné skupině či uživateli

- f. U atributu **msDS-PasswordReversibleEncryptionEnabled** zadejte do pole **Value** hodnotu **False** a pokračujte **Next >**
    - Atribut **msDS-PasswordReversibleEncryptionEnabled** určuje, zda mají být hesla ukládána pomocí reverzibilního šifrování
  - g. U atributu **msDS-PasswordHistoryLength** zadejte do pole **Value** hodnotu **0** a pokračujte **Next >**
    - Atribut **msDS-PasswordHistoryLength** udává, kolik naposledy zadaných hesel nesmí uživatel použít při změně hesla
  - h. U atributu **msDS-PasswordComplexityEnabled** zadejte do pole **Value** hodnotu **True** a pokračujte **Next >**
    - Atribut **msDS-PasswordComplexityEnabled** určuje, zda jsou vyžadována silná hesla
  - i. U atributu **msDS-MinimumPasswordLength** zadejte do pole **Value** hodnotu **3** a pokračujte **Next >**
    - Atribut **msDS-MinimumPasswordLength** určuje minimální délku hesel
  - j. U atributu **msDS-MinimumPasswordAge** zadejte do pole **Value** hodnotu **0:00:00:00** a pokračujte **Next >**
    - Atribut **msDS-MinimumPasswordAge** určuje, za jakou dobu je možné nejdříve změnit heslo ve formátu **<dny>:<hodiny>:<minuty>:<sekundy>**
  - k. U atributu **msDS-MaximumPasswordAge** zadejte do pole **Value** hodnotu **90:00:00:00** a pokračujte **Next >**
    - Atribut **msDS-MaximumPasswordAge** určuje, za jakou dobu vyprší platnost hesla ve formátu **<dny>:<hodiny>:<minuty>:<sekundy>**
  - l. U atributu **msDS-LockoutThreshold** zadejte do pole **Value** hodnotu **5** a pokračujte **Next >**
    - Atribut **msDS-LockoutThreshold** udává, po jakém počtu špatně zadaných hesel dojde k zablokování účtu
  - m. U atributu **msDS-LockoutObservationWindow** vložte do pole **Value** hodnotu **0:01:00:00** a pokračujte **Next >**
    - Atribut **msDS-LockoutObservationWindow** udává, kdy dojde k vynulování počítadla špatně zadaných hesel ve formátu **<dny>:<hodiny>:<minuty>:<sekundy>**
  - n. U atributu **msDS-LockoutDuration** vložte do pole **Value** hodnotu **1:00:00:00** a pokračujte **Next >**
    - Atribut **msDS-LockoutDuration** udává délku zablokování účtu, pokud bylo několikrát zadáno špatné heslo, ve formátu **<dny>:<hodiny>:<minuty>:<sekundy>**
  - o. Potvrďte vytvoření PSO objektu pomocí **Finish**
    - V případě výskytu chyby **Operation failed. error code: 0x20e7, The modification was not permitted for security reasons.** ověřte správně zadané hodnoty výše, tato chyba nastává v případě nemožnosti zpracovat zadané hodnoty **ADSI Edit** konzolí
5. Aplikujte PSO objekt **Simpsons PSO** na uživatele ze skupiny **Simpsons**
- a. Klikněte pravým na objekt **CN=Simpsons PSO** a zvolte **Properties**
  - b. Na záložce **Attribute Editor** vyberte atribut **msDS-PSOAppliesTo** a zvolte **Edit**
  - c. Zvolte **Add Windows Account...**
  - d. Do **Enter the object names to select** zadejte **Simpsons** a zvolte **Check Names**
  - e. Potvrďte třikrát pomocí **OK**

6. Zjistěte, který PSO objekt má být aplikován na uživatele homer
  - a. Otevřete **ADUC** (*Active Directory Users and Computers*)
    1. **Start** → **Administrative Tools** → **Active Directory Users and Computers**
  - b. Zapněte zobrazení pokročilých vlastností uživatelských účtů
    1. V menu konzole vyberte **View** a zvolte **Advanced Features**
  - c. Klikněte pravým na uživatele **homer** a zvolte **Properties**
  - d. Přejděte na záložku **Attribute Editor**
  - e. Zvolte **Filter** níže a vyberte **Constructed** pod **Show read-only attributes**
  - f. Vyhledejte v seznamu atribut **msDS-ResultantPSO** a ověřte, že obsahuje **CN=Simpsons PSO,CN=Password Settings Container,CN=System,DC=testing,DC=local**
7. Zkuste nastavit uživateli **homer** nové heslo **bbb**
  - a. Klikněte pravým na uživatele **homer** a zvolte **Reset Password...**
  - b. Zadejte heslo **bbb**
    - Heslo nepůjde vytvořit, jelikož **Simpsons PSO** vyžaduje silná hesla