Konfigurace Active Directory Domain Services ve Windows Server 2019

cvičení 5

Fakulta Informatiky a Managementu

Univerzita Hradec Králové

Ing. David Šec (david.sec@uhk.cz),

Ing. Tomáš Svoboda, Ph.D. (tomas.svoboda@uhk.cz)

leden 2021

1 Seznam úkolů

1. Vytvořte v Active Directory následující strukturu:
   - Hradec Králové
     - OS1a Servers
     - OS1a Computers
     - OS1a Users
       - Marketing
       - Sales
       - Management
     - OS1a Admins

2. Přesuňte počítač WIN_SERVER_2019_2 do organizační jednotky OS1a Computers.

3. Vytvořte uživatele v následujících organizačních jednotkách:
   - Karel Novák login: *user001* Marketing
   - Jan Novotný login: *user002* Sales
   - Michal Černý login: *user003* Management
   - „Vaše jméno“ login: *admin* OS1a Admins

4. Zakažte přihlášení uživatele Karel Novák.

5. Pokuste se vícenásobně přihlásit s účtem Jan Novotný, aby se tento účet zablokoval.

6. Odemkněte účet Jan Novotný, změňte uživateli heslo, nastavte vynucenou změnu hesla při
dalším přihlášení.

7. Nastavte uživateli Michal Černý, že se může přihlásit jen v určitý čas.

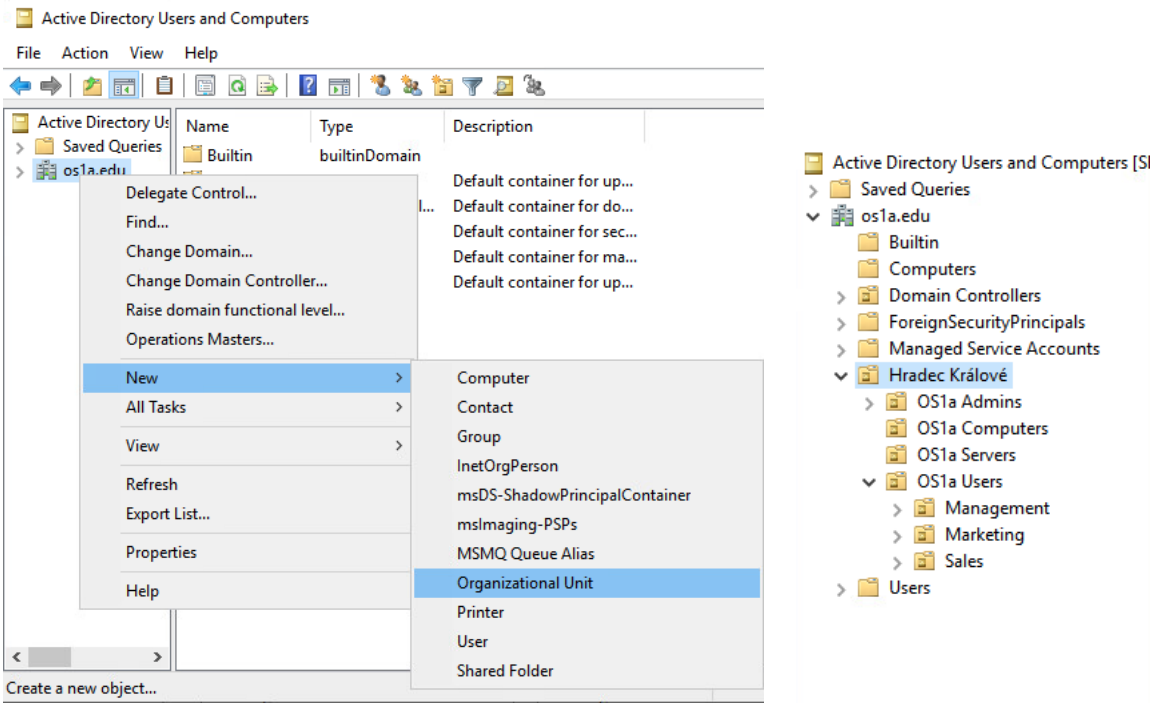
8. Delegujte na Vašeho uživatele právo spravovat organizační jednotku OS1a Users.

9. Vytvořte uživatele Marek Beneš, který bude členem skupiny Marketing a zároveň členem skupiny Sales. Jak byste toho docílili v malém prostředí a jak v obrovském prostředí?

2 Postup řešení

2.1 Vytvoření základní struktury OU

Na serveru WIN_SERVER_2019 otevřeme v Server Manageru položku Active Directory Users and Computers. Na serveru OS1a.edu vytvoříme následující organizační jednotky volbou New → Organizatonal Unit s názvem *Hradec Králové*. V ní následně stejným způsobem vytvořte kompletní strukturu organizace dle zadání (Obrázek 1).



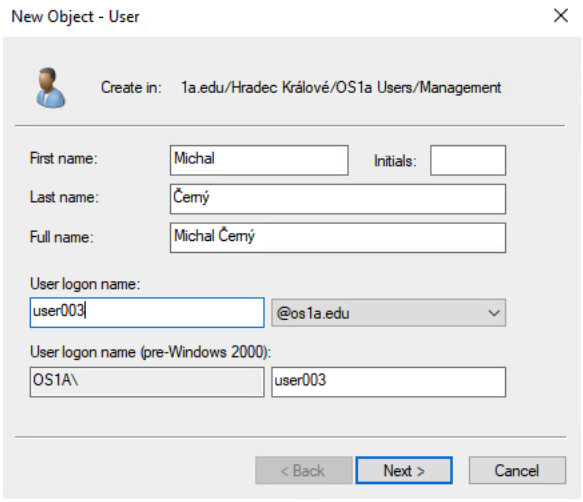
Obrázek 1: Vytvoření základní struktury organizační jednotky (OU)

2.1.1 Přesunutí počítače WIN_SERVER_2019_2 do OU OS1a Computers

V položce vyhledáme druhý počítač WIN_SERVER_2019_2 (název se může lišit) , který jsme na minulém cvičení přesunuli do domény a přetažením myši jej přesuneme do OU OS1a Computers. Na tuto skupinu lze později aplikovat pravidla, která se následně projeví na všech počítačích v této složce. To si však ukážeme až v následujících cvičeních.

2.1.2 Vytváření uživatelů

Nového uživatele můžeme vytvořit poklepáním na ikonu  v příslušné OU, případně přes pravé tlačítko myši New → User. Následně vyplníme údaje o uživateli a v dalším kroku nastavíme heslo pro přihlášení. V aktuálních politikách pro volbu silného hesla je požadavek na alespoň jeden speciální znak, proto jako heslo zvolíme například: FimUHK2021! a volbu potvrdíme. To to jakým způsobem lze změnit požadavky na sílu hesla si opět ukážeme příště.



Obrázek 2: Vytvoření nového uživatele

Pro přidání několika jednotek uživatelů je tento způsob ještě snesitelný, ale případě importu několika stovek uživatelů by jejich ruční zadávání asi nebyl nejlepší způsob. Proto si nyní ukážeme, jakým způsobem lze importovat uživatele hromadně pomocí konzole PowerShell.

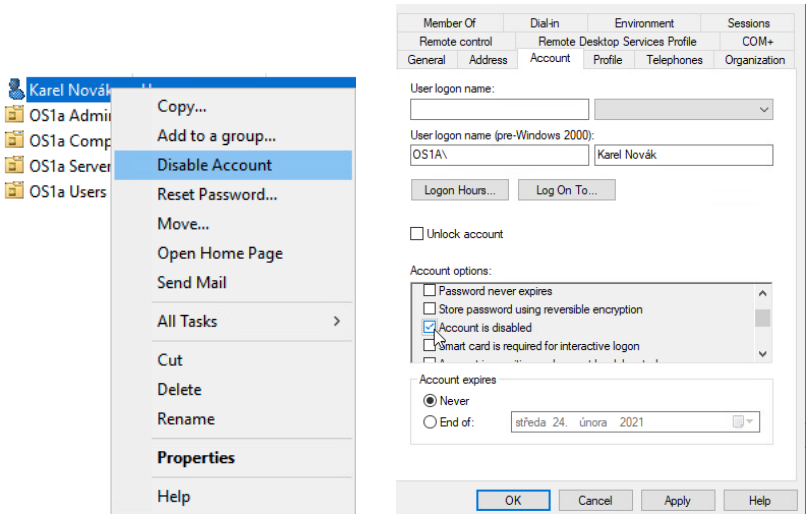
```
New-ADUser -Name "Karel Novák" -GivenName "Karel" -Surname
"Novák" -AccountPassword(Read-Host -AsSecureString
"TopSecr3tPassword#") -Enabled $true -ChangePasswordAtLogon
$true -Path "OU=Hradec Králové,DC=os1a,DC=edu"
```

Případně s požadavkem na specifikaci hesla do konzole:

```
New-ADUser -Name "Karel Novák" -GivenName "Karel" -Surname
"Novák" -AccountPassword(ConvertTo-SecureString
"TopSecr3tPassword#" -AsPlainText -Force) -Enabled $true
ChangePasswordAtLogon $true -Path "OU=Hradec
Králové,DC=os1a,DC=edu"
```

Příkazy nyní zkoušet nemusíte, ale věřím, že v budoucnu Vám ušetří spoustu námahy.

V následujícím kroku zkuste deaktivovat uživatele Karel Novák. To lze učinit buď volbou Disable Account po kliknutí pravým tlačítkem na uživatele, nebo ve vlastnostech uživatele na kartě Accounts v okně Account Options.



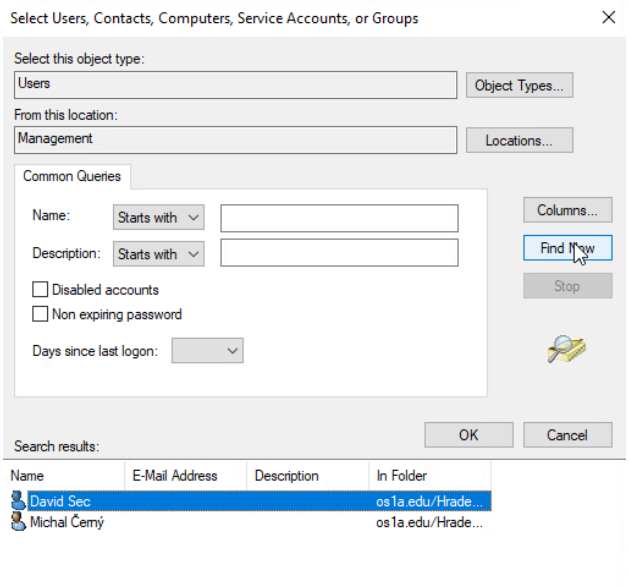
Obrázek 3: Deaktivace už. Účtu

Dále si se můžete zkusit přihlásit se pod stejným uživatelským účtem na několika počítačích zároveň, případně zkuste opakovaně vyplnit špatné heslo tak, aby se daný účet zablokoval. Poté účet odemkněte a nastavte vynucenou změnu hesla při dalším přihlášení.

Na stejné kartě můžeme rovněž nastavit uživateli vybraný čas, kdy se může přihlásit. Nastavíme tedy uživateli Karel Novák čas pro přihlášení pouze od 8 do 16 hodin.

2.1.1 Vytváření skupin

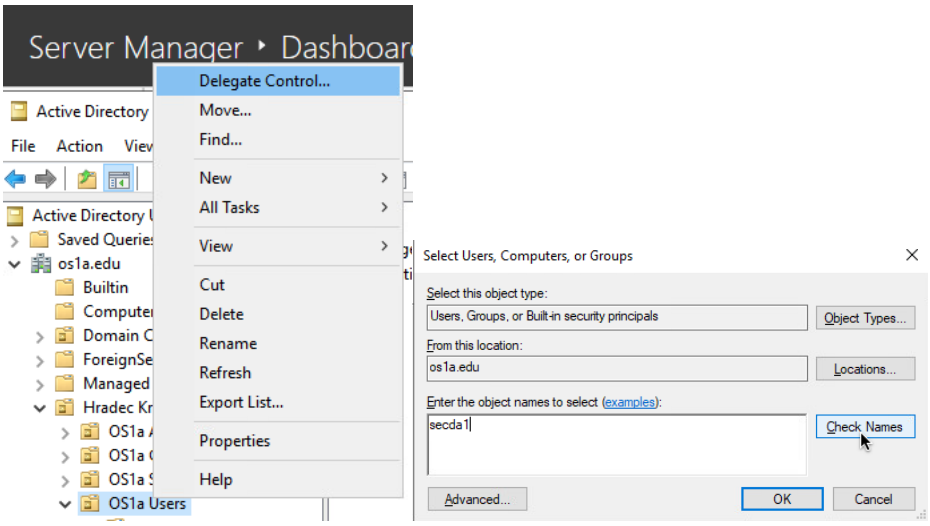
V OU Management, Marketing a Sales bychom ještě měli vytvořit skupiny se shodným názvem, ke kterým lze následně přiřadit jednotlivé uživatele pomocí ikony . Následně přidáme uživatele v dané OU jako členy těchto skupin. To lze buď ručně po jednom volbou *Add to Group* po kliknutí pravým tlačítkem na uživatele. Druhý způsob je přidat několik uživatelů najednou volbou *Add* na kartě *Members* ve Vlastnostech dané skupiny a následně s volbou *Advanced* vyfiltrovat pouze uživatele v dané lokalitě stejně jako na Obrázku 4. Následně lze označit několik uživatelů naráz a volbou *OK* přidat jako členy dané skupiny.

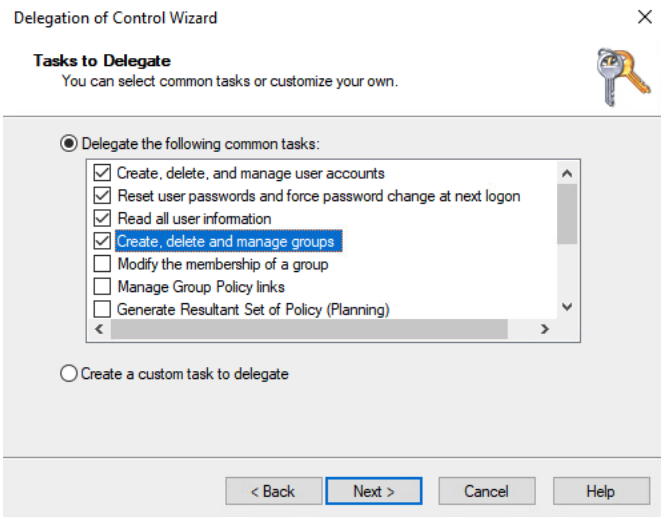


Obrázek 4: Přidání uživatelů do skupiny

2.1.2 Delegace práv OU

Organizační jednotky mohou spravovat odpovídající uživatelé, kteří k tomu dostali odpovídající práva. V následujícím kroku delegujeme právo spravovat organizační jednotku OS1a Users uživateli s vaším jménem. To provedeme po kliknutí parvým tlačítkem na danou OU volbou *Delegate Control*, nebo ve vlastnostech dané OU na kartě Managed by. Uživatele vyhledáme zadáním loginu a volbou Check Names ověříme daného uživatele. Případně lze využít kartu Advanced a uživatele vyhledat. Uživateli přidělíme práva na Správu uživatelů i skupin, resetování hesel a zobrazení kompletních informací o jednotlivých uživatelích (viz Obrázek 5).





Obrázek 5: Delegace práv pro správu OU uživateli

Vytvořte uživatele Marek Beneš, který bude členem skupiny Marketing a zároveň členem skupiny Sales.

K zamyšlení: Jak byste toho docílili v malém prostředí a jek byste toho docílili v obrovském Prostředí se stovkami uživatelů?

Můžeme přidat uživatele do obou skupin, nebo přidat uživatele pouze do jedné skupiny (nebo využít některou z již existujících) a tu přidat do skupiny druhé. Vyzkoušejte si přidání uživatele do skupiny přes vlastnosti uživatele, následně přes vlastnosti skupiny a na závěr si zkuste přidat skupinu jako člena jiné skupiny.