Windows Server 2019

jako File Server

cvičení 7

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 složku C:/shared a tuto složku nasdílejte.

2. Nastavte práva tak, aby měl uživatel user001 právo editovat soubory, user002 právo číst soubory a uživatel user003 neměl do složky žádný přístup.

3. Vytvořte složku *C:/shared/admins*, do které budou mít oprávnění pouze uživatelé Administrators v AD (pozor, nikoliv lokální Administrators).

4. Zakažte dědění oprávnění pro tuto složku.

5. Zjistěte, jaký je rozdíl mezi právy ke sdílení a NTFS právy.

6. Vytvořte složku C:/hidden_share, která bude nasdílená ale nebude vidět mezi ostatními nesdílenými složkami na serveru.

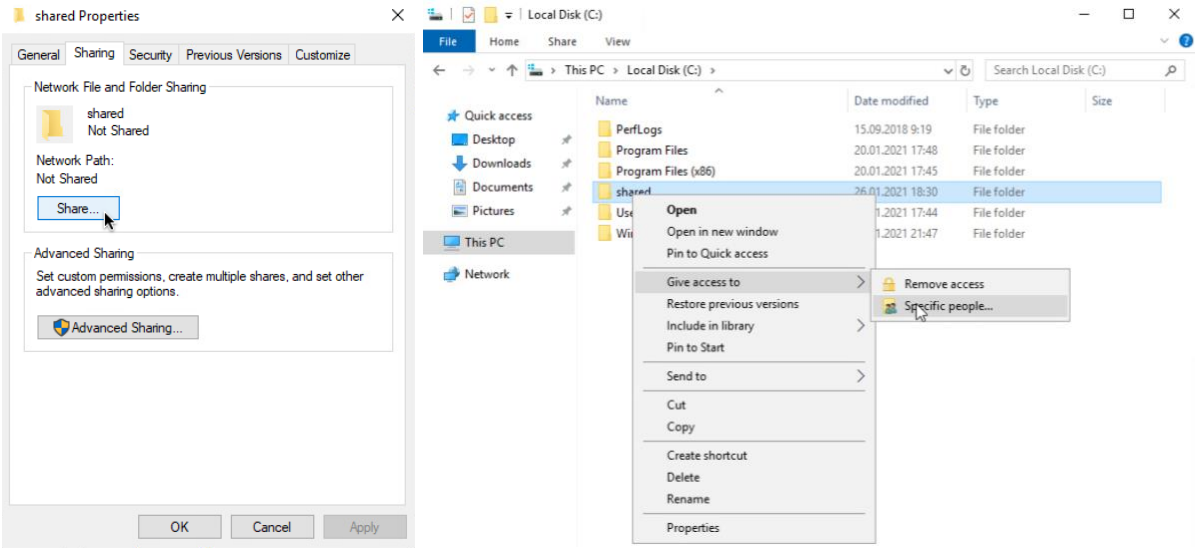
7. Vytvořte složku C:/shared_limited do které budou mít oprávnění zapisovat všichni uživatelé ale maximálně 100 MB na uživatele, tedy omezte uživatele diskovou kvótou na 100 MB.

8. Otestujte vložení velkého souboru do složky v předcházejícím úkolu

2 Postup řešení

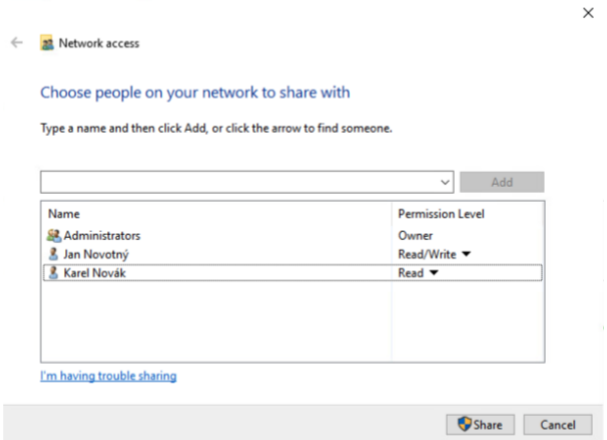
2.1 Sdílená složka

Nejprve je nutné standardním způsobem vytvořit složku *Shared* na disku C:\ a následně ji nasdílet přes Vlastnosti složky na kartě Sharing, případně volbou *Give access to* po kliknutím pravým tlačítkem na složku (Obrázek 1).



Obrázek 1: Sdílení složky

Následně jíž stačí vyhledat požadované uživatele a nastavit jim práva dle zadání stejně jako na Obrázku 2. Stejným způsobem si můžete zkusit přiřadit přístupová práva určité skupině, případně si vytvořte novou skupinu. Po nastavení sdílení prozkoumejte možnosti karty *Security* ve Vlastnostech dané složky, případně zde zkuste práva modifikovat.



Obrázek 2: Výběr uživatelů a přiřazení přístupových práv

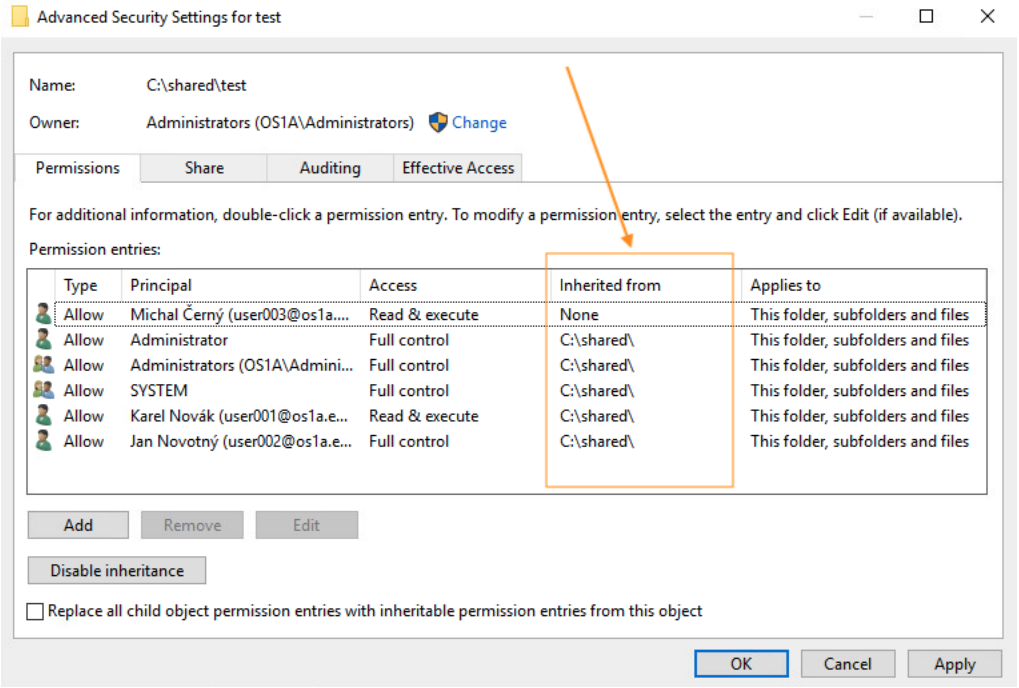
Uvnitř složky shared vytvoříme další podadresář *Admins* do které budou mít přístup pouze členové skupiny Administrators. Cesta k této složce tedy bude:

C:\Shared\Admins

To provedeme stejným způsobem jako v předchozím případě, povšimněte si však, že se zde opět nachází uživatelé user001 a user 002.To je způsobeno tím, že tito uživatelé mají přístup k nadřazené složce a mají automaticky (poděděný) přístup i ke všem podložkám v daném adresáři. My je však v tuto chvíli odebereme.

2.2 Dědění oprávnění (Inheritance)

Jak již bylo zmíněno, tak podadresáře mohou dědit přístupová práva z nadřazeného adresáře. Dědičnost lze ověřit ve vlastnostech složky na kartě *Security* pod tlačítkem *Advanced*.
To, ze kterého adresáře je přístup poděděn lze ověřit ve sloupci *Inherited from* vyznačeném na Obrázku 3. Poděděné atributy lze upravovat vždy pouze v nadřazených adresářích uvedených v tomto sloupci.



Obrázek 3: Inheritance

Nyní si zkuste dědičnost pro danou složku deaktivovat tlačítkem *Disable inheritance*.
Pokud dědičnost zakážeme, systém se následně zeptá, co se má stát se zděděnými položkami. My provedeme jejich odstranění volbou *Remove all inherited permissions from this object.*

2.3 Práva sdílení vs NTFS práva

Přístupová práva lze definovat formou práv sdílení na kartě Sharing, nebo formou NTFS práv na kartě Securtity. Pro zajištění správného nastavení oprávnění u uživatelů je třeba znát rozdíl mezi oprávněními pro sdílení a NTFS.

Oprávnění ke sdílení a NTFS fungují zcela odděleně od sebe navzájem, ale nakonec slouží stejnému účelu: zabránit neoprávněnému přístupu. Jednou z běžných otázek, které se objevují při konfiguraci zabezpečení, je „co se stane, když se vzájemně ovlivňují oprávnění sdílení a NTFS?“ Pokud společně používáte oprávnění sdílení a NTFS, vyhrává „nejpřísnější“ oprávnění. Uveďme si příklad, kdy formou práv sdílení nastavíme uživateli právo pouze číst danou složku, ale zároveň stejnému uživateli formou NTFS práv povoláme úplné řízení (čtení, zápis, úpravy, vylistovat obsah složky…). V takovém případě bude uživateli pořád umožněno pouze číst danou složku.

Pokud zjistíte, že práce se dvěma samostatnými sadami oprávnění je příliš komplikovaná nebo časově náročná na správu, můžete přepnout na používání pouze oprávnění NTFS. Kromě toho oprávnění NTFS platí bez ohledu na to, zda je ke zdroji přistupováno místně nebo prostřednictvím sítě.

2.4 Skrytá sdílená složka (Hidden Share)

Zadání: Vytvořte složku C:/hidden_share, která bude nasdílená ale nebude vidět mezi ostatními nasdílenými složkami na serveru.

Jako alternativa ke Správě sdílení nabízí sdílení souborů pod Windows rovněž tzv. skryté sdílení. Jedná se o možnost, kdy není sdílený adresář viditelný v seznamu sdílených položek (a to ani vlastníkovy této položce) ale zároveň je volně přístupný, pokud známe jeho jméno.

Hidden Share můžeme vytvořit pridáním znaku „$“ na konec názvu položky. Pro přístup k takové položce stačí do pole adresa napsat:

\\ComputerName\hiddenShareName$,

kde *ComputerName* značí identifikátor stanice v síti (nejčastěji IP adresu, nebo název stanice) a *hiddenShareName* název skryté sdílené složky včetně znaku „$“. V našem případě tak bude adresa pro přístup ke skryté složce vypadat například takto:

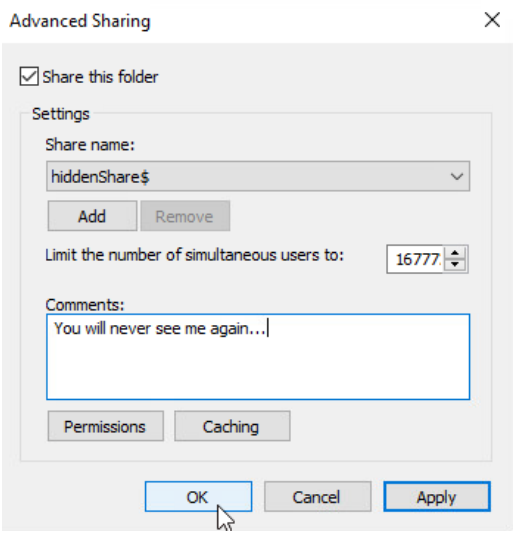
\\10.0.0.1/ *hidden_share$*

I když Hidden Share poskytují falešný pocit bezpečí, jsou poměrně známou metodou a mohou být odhaleny celou řadou nejrůznějších utilit dostupných na internetu. V žádném případě se nedoporučuje použití skrytých sdílených složek jako ochrana citlivých údajů. Za tímto účelem jsou ve Windows dostupné například *Password Protected Sharing*, tedy sdílení chráněné heslem.

(vice např.na: https://www.tenforums.com/tutorials/49827-turn-off-password-protected-sharing-windows-10-a.html)

Postup pro vytvoření hiddenShare je následující:

- Vytvoříme tedy novou složku s názvem hidden_share a nasdílíme ji stejným způsobem jako v prvním bodě.
- Ve vlastnostech složky přejdeme na kartu Sharing a vybereme volbu Advanced Sharing.
- Nyní změníme název hidden_share na hidden_share$
- Potvrdíme a zkontrolujeme přístup k položce.



Obrázek 4: Skrytá sdílená složka

2.5 Diskové kvóty

Zadání: Vytvořte složku C:/shared_limited do které budou mít oprávnění zapisovat všichni uživatelé ale maximálně 100 MB na uživatele, tedy omezte uživatele diskovou kvótou.

Diskové kvóty nejsou jen jednoduchým omezením diskového prostoru. Po správné konfiguraci jsou uživatelé omezování ve svém užívání hned několika způsoby:

Hard limit – Pevná mez. Uživateli se nikdy nepodaří na disk uložit více, než je uvedeno v parametru.

Soft limit – "Nezávazná mez" - uživatel může uložit na disk i více, ale při překročení této meze dostane od systému varování.

Inodes, Blocks – Kvóty lze nastavit jak na celkový objem dat na disku, tak na počet souborů.

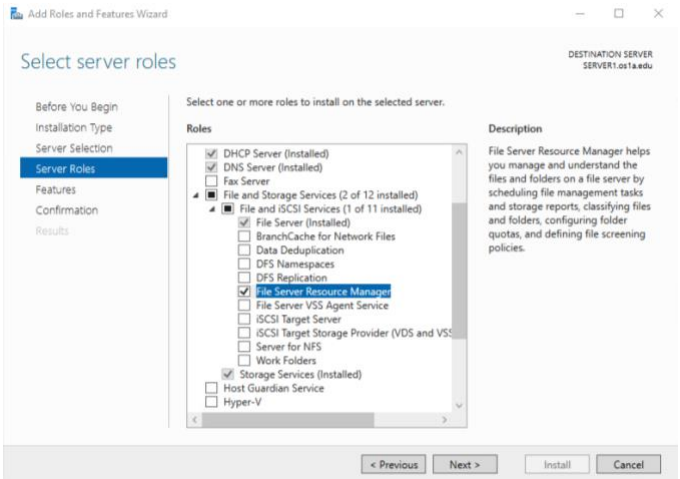
Grace period – Uživatel může dočasně uložit na disk více, než je uvedeno v parametru "soft limit" na dobu zadanou parametrem "grace period". Po uplynutí této doby se uživateli nepodaří na disk uložit více, i když ještě nepřekročil mez zadanou parametrem "hard limit".

Limity lze pochopitelně nastavovat pro každého uživatele nebo skupinu uživatelů zvlášť.

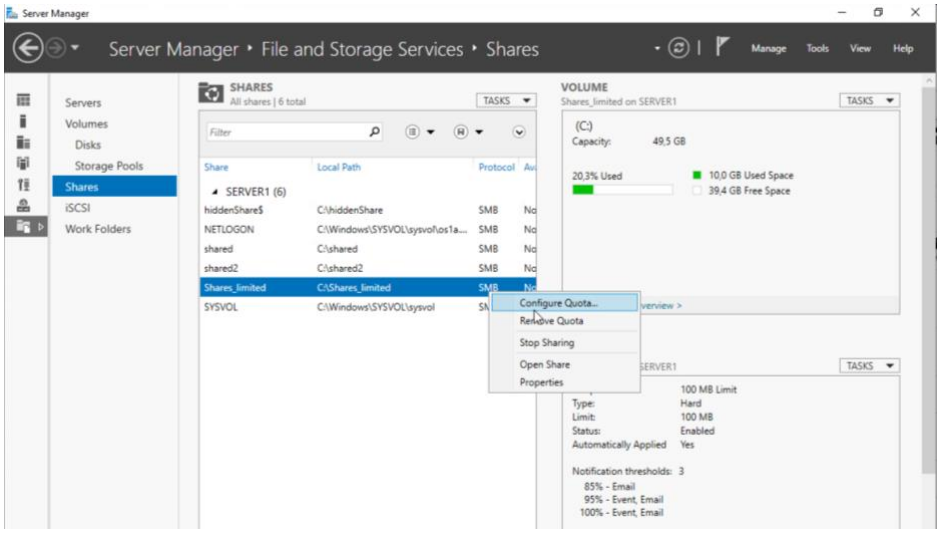
Omezit lze jak celkovou velikost souborů, tak i jejich maximální počet.

- Pro přidání diskových kvót je nezbytné přidat novou Roli *File Server Resource Manager* (viz Obrázek 5).
- Po dokončení instalace přejdeme v Server manager v levé nabídce na volbu File and Storage Services.
- Přejdeme na volbu Shares a vybereme sdílenou složku shared_limited.
- Novou kvótu vytvoříme kliknutím pravým tlačítkem na tuto sdílenou složku pod volbou *Configure Quota* (viz Obrázky 6 a 7).

Otestujte nastavení, tak že se do této složky pokusíte nahrát více než povoluje disková kvóta. Pro ověření stačí zkopírovat do složky shared_limited libovolný soubor, nebo složku větší než 100 MB (např. C:\Windows\Fonts).



Obrázek 5: Instalace role File Server Resource Manager



Obrázek 6: Vytvoření diskové kvóty

Obrázek 7: Nastavení kvóty