Instytut Sterowania i Systemów Informatycznych
Uniwersytet Zielonogórski

Systemy operacyjne

Laboratorium

Zarządzanie dostępem do zasobów przy wykorzystaniu grup w Windows 7

1 Cel ćwiczenia

Ćwiczenie ma na celu praktyczne zapoznanie się z systemem Windows 7 w zakresie tworzenia rożnych rodzajów grup użytkowników oraz określania uprawnień do zasobów. Ponadto ćwiczenie obejmuje zarządzanie danymi na partycjach NTFS.

2 Podstawowe pojęcia

- **Grupa**

  Jest to zbiór kont użytkowników o takich samych prawach zabezpieczeń. Grupy użytkowników są czasami nazywane *grupami zabezpieczeń*. Poprzez grupę można przypisać uprawnienia do określonych zasobów. Użytkownik przypisany do grupy dziedziczy wszystkie prawa i uprawnienia przyznane grupie. Konto użytkownika może należeć do wielu grup

- **Grupa robocza**

  Podczas konfigurowania sieci system Windows automatycznie tworzy grupę roboczą i nadaje jej nazwę `WORKGROUP` lub `GRUPA_ROBOCZA`. Można przyłączyć się do grupy roboczej istniejącej w sieci lub utworzyć nową.

  Grupy robocze zapewniają podstawowe funkcje udostępniania plików i drukarek, ale nie konfigurują ustawień udostępniania. W Windows 7 można utworzyć *grupę domową* lub przyłączyć się do niej, co powoduje automatyczne włączenie funkcji udostępniania plików i drukarek w sieci domowej. W przypadku korzystania z sieci domowej zalecamy utworzenie grupy domowej lub przyłączenie się do niej.

  Właściwości komputerów w grupie roboczej:

  – Wszystkie komputery są równorzędne; żaden komputer nie ma kontroli nad innym.
  – Każdy komputer ma zestaw kont użytkownika. Aby zalogować się na dowolnym komputerze należącym do grupy roboczej, trzeba mieć na tym komputerze konto.
  – Grupa robocza zawiera na ogół nie więcej niż dwadzieścia komputerów.
  – Dostęp do grupy roboczej nie jest chroniony hasłem.
  – Wszystkie komputery muszą znajdować się w tej samej sieci lub podsieci lokalnej.

  Jak sprawdzić do jakiej grupy należę – właściwości `Komputer` → `Zmień ustawienia` i odczytać co znajduje się przy napisie '*Grupa robocza:*'.

- **Active Directory (AD)**

  Usługa katalogowa w systemie Windows przechowująca informacje o zasobach (takich jak drukarki, użytkownicy, komputery i grupy) i udostępniająca je użytkownikom i administratorom sieci.

- **Kontroler domeny**

Serwer w sieci usługi Active Directory zarządzający logowaniem się i dostępem użytkowników do sieci i udostępnianych zasobów.

W domenie:

- Co najmniej jeden komputer to serwer. Za pomocą serwerów administratorzy sieci kontrolują zabezpieczenia i uprawnienia dla wszystkich komputerów w domenie. W ten sposób można łatwo wprowadzać zmiany, ponieważ są one automatycznie wdrażane na wszystkich komputerach. Zawsze, gdy użytkownicy domeny uzyskują do niej dostęp, muszą podawać hasło lub inne poświadczenia.
- Mając konto użytkownika w domenie, można logować się na dowolnym komputerze w domenie, nie posiadając na tym komputerze konta.
- Najczęściej dokonywanie zmian ustawień na komputerze przez użytkowników możliwe jest tylko w ograniczonym zakresie, ponieważ administratorzy sieci zwykle chcą zapewnić spójność we wszystkich komputerach.
- W domenie mogą być tysiące komputerów.
- Komputery mogą być z różnych sieci lokalnych

- **Grupa w grupie roboczej**

  - tworzona jest na komputerach, które nie są kontrolerami domeny
  - nie można jej utworzyć na kontrolerze domeny, gdyż nie posiada on niezależnej od Active Directory bazy danych zabezpieczeń (a taką bazą jest właśnie SAM (ang. *Security Account Manager*))
  - informacje o nich przechowywane są w SAM, która jest lokalną bazą danych informacji o zabezpieczeniach komputera
  - informacje o nich nie są umieszczane w Active Directory
  - wykorzystywane są do przypisywania uprawnień do zasobów i praw do wykonywania zadań systemowych na komputerach, na których są tworzone

  W grupie roboczej mogą być tworzone tylko grupy lokalne. Grupy te mogą zawierać lokalne konta użytkowników, jak również konta i grupy z domeny, do której należy komputer. Grupy nie mogą być członkami innych grup. Nowe grupy mogą być tworzone przez użytkowników należących do grupy `Administratorzy`.

- **Wbudowane grupy lokalne**

  Członkowie tych grup posiadają prawa do wykonywania zadań systemowych. Występują na wszystkich komputerach pracujących pod kontrolą systemu Windows. Tworzone są podczas instalacji systemu. Nie można ich usuwać lecz można zmienić ich nazwę.

Opis ćwiczenia

1. Wykorzystanie grup

   Grupa w domenie:

   - tworzona wyłącznie w kontrolerze domeny,
   - domyślnie mogą być tworzone wyłącznie przez członków należących do grupy `Administratorzy`
   - administrator może nadać również innym użytkownikom prawo tworzenia grup
   - informacje przechowywane są w Active Directory
   - przypisywanie uprawnień do zasobów i praw do wykonywania zadań w dowolnym komputerze w domenie

   Rodzaje grup przechowywanych w Active Directory

   - dystrybucyjna – służy tylko jako lista użytkowników, nie można w niej przydzielać praw. Część oprogramowania współpracuje tylko z nimi,

- bezpieczeństwa – właściwości grupy dystrybucyjnej powiększone o możliwość przydzielania uprawnień

Zakres grup
Określa, gdzie grupa może być użyta w środowisku domenowym oraz ewentualną możliwość ich zagnieżdżania. Zakres grup może być następujący:

(a) `Globalna` – użytkownicy o podobnych wymaganiach w dostępie do sieci; mogą do nich należeć konta użytkowników i innych grup globalnych tylko z domeny, w której dana grupa jest tworzona; mogą być dodawane do innych grup globalnych, uniwersalnych i domenowych grup lokalnych; zasoby mogą znajdować się w dowolnej domenie,

(b) `Lokalna` – określenie praw dostępu do zasobów w określonej, jednej domenie; członkostwo w tych grupach nie podlega żadnym ograniczeniom; nie mogą być zagnieżdżone, nawet w ramach tej samej domeny; zasoby muszą znajdować się w tej samej domenie, nie koniecznie jednak w samym kontrolerze domeny,

(c) `Uniwersalna` – kontrolery domeny pracują pod kontrolą systemu Windows; członkostwo nie podlega żadnym ograniczeniom; grupy mogą być zagnieżdżone w innych domenowych grupach lokalnych i grupach uniwersalnych w dowolnej domenie,

Strategia wykorzystania grup w pojedynczej domenie

(a) Utworzyć i umieścić użytkowników w grupie globalnej
(b) W każdej domenie utworzyć grupy lokalne odpowiedzialne za uprawnienia do zasobów w tej domenie
(c) Określić uprawnienia grupy lokalnej (a więc jej zasobów)
(d) Przypisać grupy globalne do lokalnych - grupa globalna może być członkiem grupy lokalnej (ale nie odwrotnie)

Charakterystyka wbudowanych grup lokalnych w systemie Windows 7

- `Administratorzy` – członkowie tej grupy mają pełną kontrolę nad komputerem i mogą przypisywać prawa użytkownika oraz uprawnienia kontroli dostępu użytkownikom według potrzeb. Konto `Administrator` jest członkiem domyślnym tej grupy. Kiedy komputer jest podłączony do domeny, grupa `Administratorzy domeny` jest automatycznie dodawana do tej grupy. Grupa ta ma pełną kontrolę nad komputerem, dlatego należy ze szczególną rozwagą dodawać do niej użytkowników. Uprawnienia:
  - uzyskiwanie dostępu do komputera z sieci,
  - dostosowanie przydziałów pamięci dla procesu,
  - zezwalanie na logowanie lokalne,
  - zezwalanie na logowanie za pomocą usług terminalowych,
  - wykonywanie kopii zapasowych plików i katalogów,
  - zmienianie czasu systemowego,
  - zmienianie strefy czasowej,
  - tworzenie pliku strony,
  - tworzenie obiektów globalnych,
  - tworzenie łączy symbolicznych,
  - debugowanie programów,
  - wymuszanie zamknięcia systemu z systemu zdalnego,
  - personifikowanie klienta po uwierzytelnieniu,
  - powyższanie priorytetu harmonogramu,
  - ładowanie i zwalnianie sterowników urządzeń,
  - logowanie w trybie wsadowym,
  - zarządzanie dziennikiem inspekcji i zabezpieczeń,
  - modyfikowanie zmiennych środowiskowych oprogramowania,
  - wykonywanie zadań związanych z konserwacją woluminów,

  - profilowanie pojedynczego procesu,
  - profilowanie wydajności systemu,
  - usuwanie komputera ze stacji dokującej,
  - przywracanie plików i katalogów,
  - zamykanie systemu,
  - przejmowanie na własność plików lub innych obiektów.
- `Operatorzy kopii zapasowych` – członkowie tej grupy mogą tworzyć kopie zapasowe plików na komputerze i przywracać je bez względu na uprawnienia chroniące te pliki. Dzieje się tak dlatego, że prawo tworzenia kopii zapasowych jest ważniejsze od wszystkich uprawnień do plików. Członkowie tej grupy nie mogą zmieniać ustawień zabezpieczeń. Uprawnienia:
  - uzyskiwanie dostępu do komputera lokalnego z sieci,
  - zezwalanie na logowanie lokalne,
  - wykonywanie kopii zapasowych plików i katalogów,
  - logowanie w trybie wsadowym,
  - przywracanie plików i katalogów,
  - zamykanie systemu.
- `Operatorzy kryptograficzni` – członkowie tej grupy są autoryzowani do wykonywania operacji kryptograficznych. Grupa nie posiada domyślnych praw użytkownika.
- `Użytkownicy DCOM` – członkowie tej grupy mogą uruchamiać i aktywować obiekty DCOM na komputerze, a także korzystać z nich. Grupa nie posiada domyślnych praw użytkownika.
- `Goście` – członkowie tej grupy mają profil tymczasowy tworzony w momencie logowania, który po wylogowaniu danego użytkownika jest usuwany. Konto `Gość` (domyślnie wyłączone) jest także domyślnym członkiem tej grupy. Grupa nie posiada domyślnych praw użytkownika.
- `IIS_IUSRS` – Wbudowana grupa używana przez Internetowe usługi informacyjne (IIS). Brak domyślnych praw użytkownika.
- `Operatorzy konfiguracji sieci` – członkowie tej grupy mogą zmieniać ustawienia TCP/IP oraz odnawiać i zwalniać adresy TCP/IP. Ta grupa nie ma członków domyślnych i nie posiada domyślnych praw użytkownika.
- `Użytkownicy dzienników wydajności` – członkowie tej grupy mogą zarządzać licznikami, dziennikami i alertami wydajności na komputerze — zarówno lokalnie, jak i z klientów zdalnych — bez przynależności do grupy `Administratorzy`. Brak domyślnych praw użytkownika.
- `Użytkownicy monitora wydajności` – członkowie tej grupy mogą monitorować liczniki wydajności na komputerze - lokalnie i z klientów zdalnych - bez przynależności do grupy `Administratorzy` lub do grup `Użytkownicy dzienników wydajności`. Grupa nie posiada domyślnych praw użytkownika.
- `Użytkownicy zaawansowani` – domyślnie członkowie tej grupy nie mają więcej uprawnień niż standardowe konto użytkownika. Grupa `Użytkownicy zaawansowani` była wykorzystywana w starszych wersjach systemu Windows, aby umożliwić przyznawanie określonych praw i uprawnień administratora do wykonywania typowych zadań systemowych. W wersji systemu Windows Vista standardowe konta użytkownika mają nieodłączną możliwość wykonywania najbardziej typowych zadań konfiguracyjnych, takich jak zmiana strefy czasowej. W przypadku starszych aplikacji, wymagających takich samych praw i uprawnień użytkownika zaawansowanego, jakie były obecne w starszych wersjach systemu Windows, administratorzy mogą zastosować szablon zabezpieczeń pozwalający założyć, że grupa `Użytkownicy zaawansowani` ma takie same prawa i uprawnienia, jakie były dostępne w starszych wersjach systemu Windows. Brak domyślnych praw użytkownika.
- `Użytkownicy pulpitu zdalnego` – członkowie tej grupy mogą zdalnie logować się na komputerze. Uprawnienia:
  - zezwalanie na logowanie za pomocą usług terminalowych.

- `Replikator` – ta grupa obsługuje funkcje replikacji. Jedynym członkiem grupy `Replikator` powinno być konto użytkownika domeny używane do logowania się w usługach Replikatora kontrolera domeny. Nie należy dodawać kont prawdziwych użytkowników do tej grupy. Brak domyślnych praw użytkownika.
- `Użytkownicy` – członkowie tej grupy mogą wykonywać typowe zadania, np. uruchamiać aplikacje, korzystać z drukarek lokalnych i sieciowych oraz blokować komputer. Członkowie tej grupy nie mogą udostępniać katalogów ani tworzyć drukarek lokalnych. Domyślnie grupy `Użytkownicy domeny`, `Użytkownicy uwierzytelnieni` i `Użytkownicy interakcyjni` są członkami tej grupy. Dlatego każde konto użytkownika utworzone w domenie zostaje członkiem tej grupy. Uprawnienia:
  - uzyskiwanie dostępu do komputera lokalnego z sieci,
  - zezwalanie na logowanie lokalne,
  - zmienianie strefy czasowej,
  - powiększanie zestawu roboczego procesu,
  - usuwanie komputera ze stacji dokującej,
  - zamykanie systemu,
- `Pomocnicy oferujący Pomoc zdalną` – członkowie tej grupy mogą oferować Pomoc zdalną użytkownikom tego komputera. Grupa nie posiada domyślnych praw użytkownika.

2. Zarządzanie danymi na partycjach z systemem plików NTFS (ang. *New Technology File System*)

   Uprawnienia w systemie plików NTFS; w systemie plików NTFS z każdym plikiem przechowywana jest lista kontroli dostępu ACL (ang. *Access Control List*). Zawiera ona wykaz wszystkich kont użytkowników, grup i komputerów, które mają zdefiniowane prawo dostępu do pliku lub folderu, łącznie z rodzajem przypisanych uprawnień.

   Uprawnienia systemu plików NTFS do folderów:

   - `Pełna kontrola` – zmiana uprawnień, przejęcie folderu na własność, usuwanie plików i folderów zawartych w folderze oraz wszelkie działania, na które zezwala dowolne inne uprawnienie NTFS do folderów
   - `Modyfikacja` – usunięcie folderu oraz wszelkie działania, na które zezwalają uprawnienia `Zapis` oraz `Odczyt i wykonanie`
   - `Odczyt i wykonanie` – przechodzenie w drzewie katalogów wewnątrz folderu oraz wszystkie czynności, na które pozwalają uprawnienia `Odczyt` oraz `Wyświetlanie zawartości folderu`
   - `Wyświetlanie zawartości folderu` – przeglądanie listy plików i folderów wewnątrz danego folderu
   - `Odczyt` – przeglądanie plików i folderów, podgląd atrybutów i uprawnień do folderu oraz identyfikacja właściciela
   - `Zapis` – zakładanie w folderze nowych plików i folderów, zmiana atrybutów folderu, podgląd uprawnień do folderu oraz identyfikacja właściciela
   - `Uprawnienia specjalne` – zobacz poniżej (sekcja **Uprawnienia specjalne**)

   Uprawnienia systemu plików NTFS do plików:

   - `Pełna kontrola` – zmiana uprawnień, przejęcie pliku na własność oraz wszystkie czynności, na które zezwala dowolne inne uprawnienie
   - `Modyfikacja` – modyfikacja i usunięcie pliku oraz wszystkie inne czynności, na które zezwalają uprawnienia `Zapis` oraz `Odczyt i wykonanie`
   - `Odczyt i wykonanie` – uruchamianie programów oraz wszystkie inne czynności, na które pozwala uprawnienie `Odczyt`
   - `Odczyt` – odczyt zawartości pliku, atrybutów i uprawnień do folderu oraz identyfikację właściciela
   - `Zapis` – nadpisanie pliku, zmiana atrybutów pliku, podgląd uprawnień do pliku i identyfikacja właściciela

- `Uprawnienia specjalne` – zobacz poniżej

Uprawnienia specjalne

Stosowane są, gdy zachodzi konieczność bardzo precyzyjnego określenia uprawnień użytkowników, zaś uprawnienia standardowe nie są wystarczające. Spośród uprawnień specjalnych najważniejsze są:

- `Zmiana uprawnień` – użytkownik ma możliwość zmiany uprawnień do pliku lub folderu. Posiadanie tego uprawnienia nie umożliwia nadania prawa `Pełna kontrola`,
- `Przejęcie na własność` – użytkownik może stać się właścicielem pliku lub folderu. Administrator posiada niejawne prawo `Przejęcie na własność` do każdego pliku i folderu.

Uprawnienia plików, a operacje dyskowe:

- plik przenoszony w ramach jednej partycji NTFS zachowuje swoje uprawnienia,
- plik kopiowany lub przenoszony z partycji dowolnego typu, dziedziczy uprawnienia katalogu nadrzędnego, w którym będzie się znajdował,
- plik kopiowany lub przenoszony na partycję innego typu niż NTFS, traci swoje uprawnienia,
- w celu skopiowania folderów (plików) w obrębie jednej lub pomiędzy partycjami NTFS, należy posiadać prawo `Odczyt` do folderu (pliku) źródłowego oraz prawo `Zapis` do folderu docelowego,
- aby przenieść foldery (pliki) w obrębie jednej lub pomiędzy partycjami NTFS, należy posiadać prawo `Modyfikacja` do folderu (pliku) źródłowego oraz prawo `Zapis` do folderu docelowego

Kompresja danych na partycjach NTFS

W systemie Windows 7 kompresji mogą podlegać tylko dane niezaszyfrowane. Możliwe jest oddzielne określanie kompresji folderu i plików. Możliwe jest więc wystąpienie sytuacji, że skompresowany folder będzie zawierał nieskompresowane pliki oraz nieskompresowany folder będzie zawierał skompresowane pliki. System plików NTFS podaje zawsze rozmiar pliku po ewentualnej kompresji. Istnieje możliwość włączenia opcji wyróżniania plików skompresowanych kolorem. System kompresji jest dla aplikacji "przezroczysty", tzn. pliki skompresowane przed udostępnieniem ich pewnej aplikacji są rozpakowywane. Po zamknięciu lub zapisaniu pliku jest kompresowany powtórnie.

Kompresja, a operacje dyskowe

- plik przenoszony w ramach jednej partycji NTFS zachowuje atrybut kompresji,
- plik kopiowany lub przenoszony z partycji dowolnego typu, dziedziczy atrybut kompresji katalogu nadrzędnego, w którym będzie się znajdował,
- plik kopiowany lub przenoszony na partycję inną, niż NTFS nie będzie kompresowany,
- kopiowanie pliku skompresowanego odbywa się trój stopniowo: rozpakowanie pliku, skopiowanie rozpakowanego pliku, kompresja pliku docelowego.

Konfiguracja przydziałów dyskowych

Przydziały dyskowe pozwalają na kontrolę ilości miejsca na dysku dla każdego użytkownika i partycji dyskowej. Wielkość zajętego obszaru dysku dla danego użytkownika można konfigurować niezależnie dla każdego użytkownika, niezależnie od tego, gdzie na dysku znajdują się jego pliki i foldery. Cechy przydziałów dyskowych są następujące:

- wykorzystanie przestrzeni dyskowej oparte jest na prawie własności do plików i folderów. Gdy użytkownik kopiuje lub zapisuje nowy plik na partycji NTFS, miejsce, które ten plik zajmuje obciąża przydział dyskowy użytkownika,
- przydział dyskowy nie uwzględnia kompresji plików. Limit jest obciążany wielkością plików nieskompresowanych, niezależnie od tego, ile miejsca zajmują faktycznie na dysku,

- ilość wolnego miejsca dostępnego dla aplikacji bazuje na limicie przydziału dyskowego,
- przydziały dyskowe kontrolowane są niezależnie dla każdej partycji NTFS, nawet, jeśli są one zlokalizowane na jednym dysku fizycznym,
- istnieje możliwość określenia limitu, którego przekroczenie spowoduje jedynie poinformowanie użytkownika o tym fakcie.

3 Przebieg ćwiczenia

1. Zalogować się jako administrator i utworzyć pięciu użytkowników o nazwach `Student1`, ..., `Student5`. Skorzystaj w tym celu z `Zarządzania komputerem`, poprzez polecenie wpisane z linii komend: `compmgmt.msc`.
2. Utworzyć dwie grupy o nazwach `Grupa1` i `Grupa2`. Do grupy `Grupa1` przypisać użytkowników `Student1`, `Student2` i `Student3`. Do grupy `Grupa2` przypisać użytkowników `Student3`, `Student4` i `Student5`.
3. Sprawdź z wiersza polecenia do jakich grup należy `Student3`. W tym cely wykonaj polecenie: `net user Student3`. Zwróć uwagę jakie informacje zostały wypisane np. o dacie ostatniego logowania. Przetestuj to polecenia dla innych kont, na których już logowanie nastąpiło.
4. Zapoznaj się z możliwością dodawania użytkowników do grypy z linii komend np. korzystając z polecenia `net localgroup GRUPA UŻYTKOWNIK /add`. W tym celu utwórz konto `Student6` z linii komend: `net user Student6 /add`, a następnie: `net localgroup Grupa1 Student6 /add`.
5. Zwróć uwagę na to, że `Student6` ma ustawione puste hasło oraz na konsekwencje, które się z tym wiążą. W tym celu zapoznaj się z zasadami `Zasady zabezpieczeń lokalnych` poprzez uruchomienie ich z poziomu `Narzędzi administracyjnych` lub wpisanie polecenia `secpol.msc`. Następnie `Ustawienia zabezpieczeń` → `Zasady lokalne` → `Opcje zabezpieczeń` → `Konta: ogranicz używanie pustych haseł przez konta lokalne tylko do logowania do konsoli`. Przeczytaj wyjaśnienia, po kliknięciu w tę zasadę.
6. Ogranicz użytkownikom z grupy `Grupa2` dostęp do komputera z sieci. W tym celu zapoznaj się z zasadą: `Zasady zabezpieczeń lokalnych` → `Ustawienia zabezpieczeń` → `Zasady lokalne` → `Przypisywanie praw użytkownika` → `Odmowa dostępu do tego komputera z sieci`. Zapoznaj się również z innymi zasadami tam zawartymi.
7. W celu zwiększenia bezpieczeństwa komputera ustaw aby nazwa ostatnio zalogowanego użytkownika nie była wyświetlana a dodatkowo wymuś aby przed zalogowaniem użytkownik musiał nacisnąć klawisze `CTRL+ALT+DEL`. W tym celu zapoznaj się z zasadami: `Zasady zabezpieczeń lokalnych` → `Ustawienia zabezpieczeń` → `Zasady lokalne` → `Opcje zabezpieczeń`:
   - `Logowanie interakcyjne: nie wyświetlaj nazwy ostatnio zalogowanego użytkownika`
   - `Logowanie interakcyjne: nie wymagaj naciśnięcia klawiszy CTRL+ALT+DEL`

   Przeczytaj uważnie wyjaśnienia na karcie: `Wyjaśnienie`.
8. Utworzyć na dysku folder o nazwie `C:\Dane_grup`. Odczytać jakie są zastosowane domyślne uprawnienia dla tak nowo utworzonego folderu na dysku `C:\`. W tym celu wykonaj: `Właściwości` na folderze `C:\Dane_grup`, karta `Zabezpieczenia`. Odczytaj jakie uprawnienia ma grupa `Użytkownicy`, `Administratorzy`. Zwróć uwagę na wpis dla `SYSTEM` oraz dla `Użytkownicy uwierzytelnieni`. Na dole tej karty znajduje się odnośnik do systemu pomocy: *Dowiedz się o kontroli dostępu i uprawnieniach.* Zapoznaj się z tą pomocą a w szczególności z hasłami:
   - *Zarządzanie uprawnieniami → Uprawnienia do plików i folderów*
   - *Interfejs użytkownika: kontrola dostępu → Okno dialogowe Wpis uprawnienia*
9. Usunąć z wszystkich z listy uprawnionych do korzystania z tego folderu. Czy możliwe jest usunięcie wszystkich grup z listy uprawnionych do korzystania z folderu `C:\Dane_grup`? Nie, dlaczego?
10. Zablokować dziedziczenie uprawnień do folderu `C:\Dane_grup`. Czy teraz jest możliwe usunięcie wszystkich z listy uprawnionych do korzystania z tego folderu? **Uwaga:** Po wykonaniu tej operacji nikt nie będzie miał praw dostępu do tego folderu. W celu rozwiązania zaistniałego problemu wykonaj następne zadanie.

11. Zmień właściciela (przjmij na własność) dla folderu `C:\Dane_grup`. W tym celu wykonaj: `Właściwości` na folderze `C:\Dane_grup`, zakładka `Zabezpieczenia` → `Zaawansowane`, zakładka `Właściciel` → `Edytuj` wybieramy administratora (lub innego właściciela poprzez wybór `Inni użytkownicy i grupy...`) i zaznaczmy pole wyboru: `Zmień właściciela dla podkontenerów i obiektów`. Tutaj też warto zapoznać się z systemem pomocy klikając w link: *Dowiedz się o własności obiektów*. Za poznaj się z poleceniem `takeown /?`.
12. Przypisać uprawnienia domyślne wraz z prawem `Zapis` do folderu `Dane_grup` grupie `Grupa1`. Przypisać grupie `Grupa2` prawa `Wyświetlanie zawartości folderu` oraz `Odczyt` i odmówić prawa `Zapis` (**uwaga:** mamy tu dwie kolumny `Zezwalaj` i `Odmów` – należy wybrać odpowiednią). Jakie są efektywne uprawnienia poszczególnych użytkowników? Zwróć szczególną uwagę na użytkownika `Student3`.
13. Sprawdź jakie prawo wynikowe ma `Student3`, gdyż w jednej grupie ma zezwolenie na `Zapis` a w drugiej nie. W tym celu wykonaj: `Właściwości` na folderze `C:\Dane_grup` karta `Zabezpieczenia` → `Zaawansowane`, karta `Czynne uprawnienia` → `Wybierz` i wybrać `Student3`. Odczytaj uprawnienia. Zapoznaj się z pomocą zawartą na dole okna poprzez link: *Jak określane są czynne uprawnienia?*
14. Zapoznaj się z poleceniem `icacls`. W tym celu uruchom wiersz polecenia i wpisz: `icacls /?`. Następnie wydaj polecenie `icacls c:\Dane_grup` by odczytać właściwości tego folderu.
15. Nadaj użytkownikowi należącemu do grupy `Administratorzy` prawo `Pełna kontrola` do folderu `Dane_grup` i utwórz plik `Admin.txt` o dowolnej treści.
16. Zaloguj się odpowiednio jako `Student1`, `Student3` oraz `Student5` i wykonaj na pliku `Admin.txt` operacje: otwarcia, zmiany zawartości, zapisu, usunięcia. Wykonanie których operacji było możliwe?
17. Zapoznać się z zaawansowanymi prawami dostępu do zasobów plikowych. `Właściwości` na folderze `C:\Dane_grup` karta `Zabezpieczenia` → `Zaawansowane`, karta `Uprawnienia` → `Zmień uprawnienia...`, wybrać jeden z wpisów uprawnień i kliknąć `Edytuj...`. Na karcie `Obiekt` przejrzeć wybrany wpis uprawnienia (można je również w tym miejscu zmienić wybierając inne uprawnienia). Proszę zwrócić uwagę, że można to uprawnienie zastosować do, poprzez wybranie listy rozwijanej nad tymi uprawnieniami `Zastosuj do:` na różne sposoby. Rozwinąć tę listę i przejrzeć ją.
18. Zalogować się jako administrator i skonfigurować program `Windows Explorer` do wyświetlania nazw skompresowanych plików i folderów w innym kolorze. Utworzyć folder `Kompresja` i skopiować do niego dowolne pliki i foldery o łącznym rozmiarze `10MB`. Podać wartości parametrów `Rozmiar` i `Rozmiar na dysku` dla tego folderu. Wyjaśnij pojęcia `Rozmiar` i `Rozmiar na dysku` – czym one się różnią i skąd wynika różnica?
19. Dokonać kompresji folderu `Kompresja`. Odczytać wartości parametrów `Rozmiar` i `Rozmiar na dysku` dla tego folderu. Porównać otrzymane wyniki z tymi uzyskanymi w poprzednim punkcie. Wyznaczyć współczynnik kompresji. W tym celu wykonaj: `Właściwości` dla folderu `Kompresja`, karta `Ogólne` → `Zaawansowane` → `Kompresuj zawartość, aby zaoszczędzić miejsce na dysku` i zatwierdzamy. Gdy pojawi się okno zatwierdzamy domyślne ustawienia.
20. Skonfigurować domyślne ustawienia przydziałów dyskowych dla dysku `C:\`, wykorzystując podane wielkości: `Ogranicz miejsce na dysku do`: 100 MB, `Ustaw poziom ostrzeżeń na`: 60 MB. Podać ilość wolnego miejsca na dysku dla administratora oraz użytkowników `Student1`, ..., `Student5`. W tym celu wykonaj: `Właściwości` dysku `C:\`, karta `Przydział` → `Włącz zarządzanie przydziałami` → `Ogranicz miejsce na dysku do` → `100` → `MB`. Warto zaznaczyć też opcję: `Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału`.
21. Zalogować się jako `Student1`. Podać ilość wolnego miejsca na dysku. Porównać z wynikami otrzymanymi w poprzednim ćwiczeniu. Skomentować rezultat.
22. Skopiować folder `C:\Windows\System32` do folderu `C:\Moje_dane`. Jaki jest rozmiar folderu `System32`? Czy możliwe było skopiowanie folderu `System32`? Odpowiedź uzasadnij.
23. Dla poszczególnych użytkowników można przydzielać różne wielkości przydziału. W tym celu należy wykonać: `Właściwości` dysku `C:`, karta `Przydział` → `Wpisy przydziałów...`, menu

`Przydział` → `Nowy wpis przydziału...`.

24. Zapoznać się z poleceniem `fsutil`. Wpisz w linii komend następujące polecenie: `fsutil fsinfo volumeinfo C:` i sprawdź czy dysk obsługuje przydziały dyskowe.
25. Sprawdzić jakie są obecnie ustawione limity przydziałów: `fsutil quota query C:`. Następnie zmodyfikować użytkownikowi `Student1` limity z 60 MB (poziom ostrzeżeń, w bajtach: $62914560 = 60 \cdot 2^{20}$) i 100 MB (limit końcowy, w bajtach: $104857600 = 100 \cdot 2^{20}$) na 80 MB (83886080 B, poziom ostrzeżeń) i 120 MB (125829120 B, limit końcowy), wydając polecenie: `fsutil quota modify C: 83886080 125829120 Student1`. Sprawdź czy operacja się powiodła: `fsutil quota query C:` a także sprawdź w trybie graficznym: `Właściwości` dysku `C:`, karta `Przydział` → `Wpisy przydziałów...` → `Nazwa logowania` → `Student1`.
26. Wyłącz przydziały dyskowe dla dysku `C:`. Który użytkownik może dokonywać tej zmiany?

4 Przykładowe pytania

1. Omówić pojęcia: grupa, grupa robocza, Active Directory, kontroler domeny, grupa w grupie roboczej.
2. Jakie mamy wbudowane grupy lokalne? Jakie uprawnienia mają poszczególne grupy?
3. Co oznacza NTFS?
4. Co oznacza ACL?
5. Omówić uprawnienia do plików i folderów.
6. Omówić przydziały dyskowe i kompresję.

Literatura

[1] Microsoft TechNet. Omówienie Systemu szyfrowania plików `http://technet.microsoft.com/pl-pl/library/cc759177(WS.10).aspx`

[2] Jim Boyce. *Windows 7 PL. Biblia.* Helion, 2010.

[3] Preppernau Joan i Cox Joyce. *Windows 7 krok po kroku.* Wydawnictwo RM, 2010.

[4] Danuta Mendrala i Marcin Szeliga. *Windows 7 PL.* Helion, 2009.

[5] Paul McFedries. *Windows 7 PL. Księga eksperta.* Helion, 2009.

[6] Andrzej Szeląg. *Windows 7 PL. Zaawansowana administracja systemem.* Helion, 2009.

[7] Witold Wrotek. *Rejestr Windows 7. Praktyczne przykłady.* Helion, 2010.