Małopolska Akademia ICT

Wprowadzenie do Active Directory. Udostępnianie katalogów

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

COMARCH

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Wprowadzenie do Active Directory.
Udostępnianie katalogów.

Prowadzący: Grzegorz Zawadzki

MCITP: Enterprise Administrator on Windows Server 2008
MCITP: Server Administrator on Windows Server 2008
MCITP: Enterprise Messaging Administrator on Exchange 2010
VMware Certified Professional
Cisco Certified Network Associate

COMARCH

Zadanie:

Firma posiada następujące działy : ***Zarząd, Księgowość, IT, Produkcja***

Zorganizować strukturę OU (jednostek organizacyjnych), użytkowników i grup.

Każdy dział będzie przechowywał **dane na serwerze w dedykowanym katalogu**.

1. Pracownicy danego działu mają mieć prawa do **zapisu i odczytu danych z katalogu swojego działu**.
2. Pracownicy poszczególnych działów **nie mogą mieć dostępu do danych innych działów**, z wyjątkiem:
   a. Pracownicy działu **zarząd powinni mieć prawo odczytu do wszystkich danych każdego z działów**.
   b. W katalogu działu IT powinien się znajdować **katalog "wersje_instalacyjne", do którego pracownicy innych działów maja mieć prawo tylko do odczytu**.
3. Zdefiniować **logon skrypty** dla użytkowników(mapowanie dysku działu na W:, mapowanie wersji instalacyjnych na Z:, dla zarządu całość danych na X:)
4. Zalogować się do stacji roboczej na pracownika każdego z działów – zweryfikować czy login skrypt wykonał się poprawnie, czy użytkownik ma odpowiedni dostęp do danych na serwerze

COMARCH

Konfiguracja

SERWER:

- System operacyjny: Windows 2008 32 bit, wersja angielska
- Zainstalowane aktualizacje Windows Update
- Kontroler Active Directory

STACJA ROBOCZA:

- System operacyjny: Windows XP 32 bit , wersja angielska
- Zainstalowane aktualizacje Windows Update
- Komputer dodany do domeny

COMARCH

Planowanie

Komponenty jakie należy rozważyć :

- Struktura OU (jednostek organizacyjnych)
- Grupy w domenie
- Użytkownicy w domenie – ich przypisanie do gru
- Struktura katalogów na dysku (system plików NTFS) + uprawnienia + mechanizm dziedziczenia
- Udostępnianie katalogów + uprawnienia
- Stworzenie i zapięcie skryptów logowania

Narzędzia:

Net use – do nawiązywania i zamykania połączenia ze stacji roboczej (weryfikacja) oraz do skryptu logowania

Share and Storage Management – do konfiguracji udziałów sieciowych

UWAGA: wyjątkowo w tym ćwiczeniu wykorzystamy kontroler domeny jako serwer plików. **W środowisku produkcyjnych NIE NALEŻY używać kontrolerów jako serwerów plików**.

COMARCH

Jednostki organizacyjne

Jednostki organizacyjne (OU - Organizational Unit) umożliwiają utworzenie hierarchii kontenerów w domenie. Służą do grupowania obiektów na potrzeby administratorów.

ORGANIZACJA – organizacja obiektów Active Directory

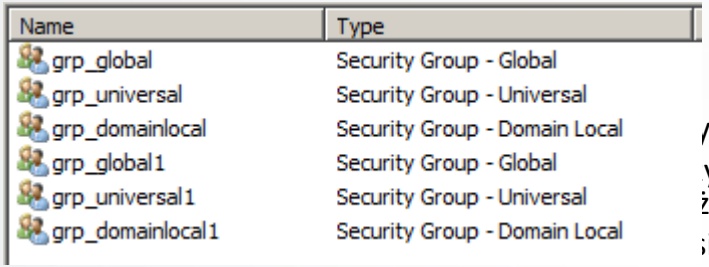
DELEGACJA UPRAWNIEŃ - Sterowanie (jednostką organizacyjną i należącymi do niej obiektami) jest określone przez listy kontroli dostępu (ACL). Za pomocą delegowania właściciele mogą w całości lub w ograniczonym zakresie przekazać kontrolę administracyjną nad obiektami innym użytkownikom lub grupom.

ZASADY GRUPY/POLITYKI (GPO - Group Policy Object) – Są zbiorami ustawień kontrolującymi zachowanie zarówno stacji klienckich jak i serwerów pod bardzo wieloma aspektami.

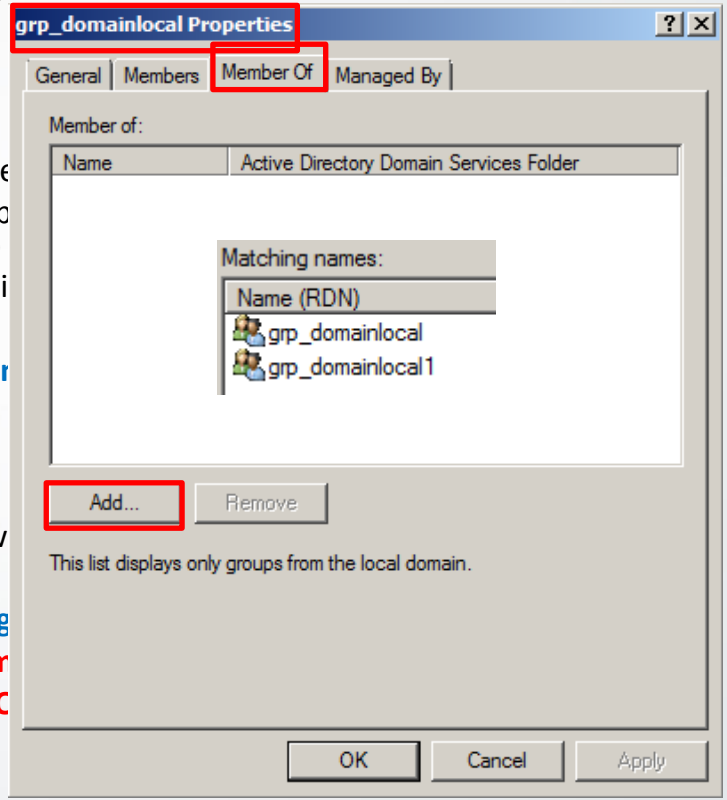
DZIEDZICZENIE – Zarówno delegacja uprawnień jak i zasady grupy podlegają mechanizmowi dziedziczenia.

COMARCH

Grupy

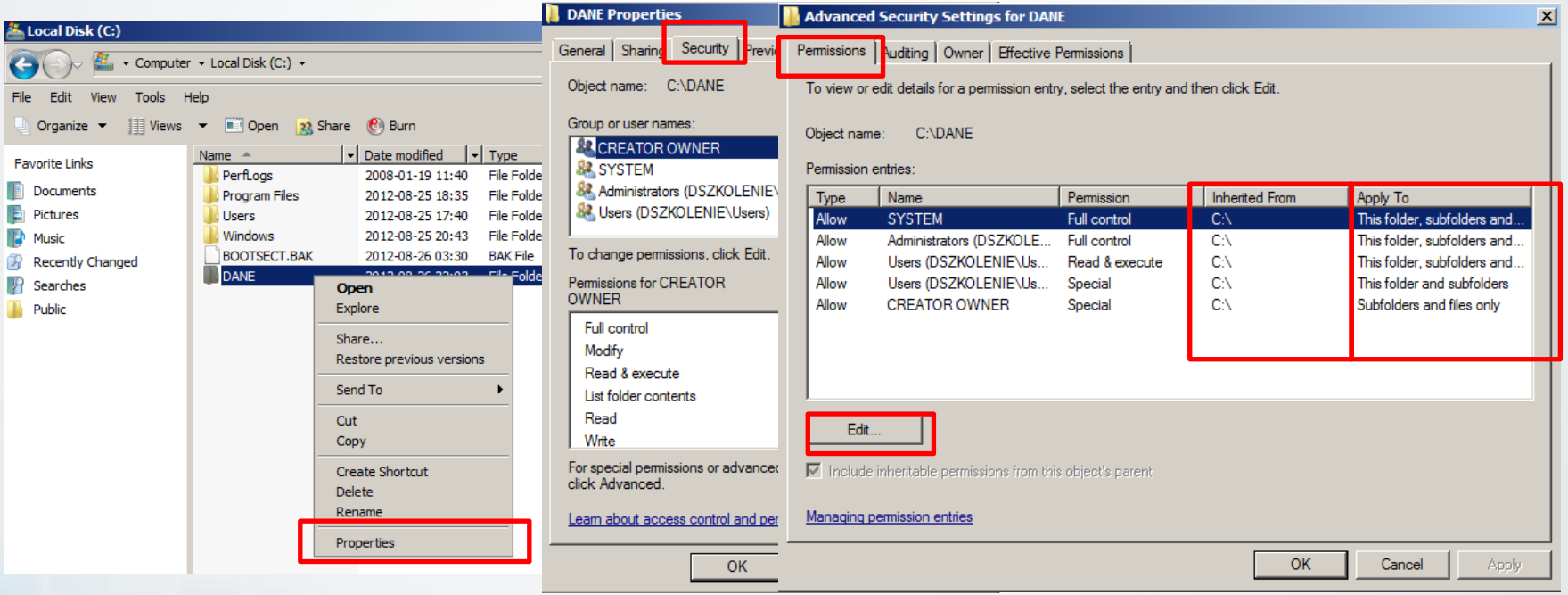


- ywamy do przedzie
- ywamy do dystryb
- żna ich używać do
- sięg obowiązywani
  - **Global:**
    - Mogą zawierać **TYLKO użytkowników i grupy globalr**
    - **NIE mogą zawierać grup Domain Local**
    - Mogą być członkami grup Universal i Domain Local.
  - **Universal:**
    - Mogą zawierać użytkowników, grupy globalne i uniw
  - **Domain Local:**
    - Mogą zawierać użytkowników, **grupy uniwersalne i g**
    - **Mogą zawierać grupy Domain Local z tej samej dom**
    - Przy ich użyciu można przydzielać dostęp **tylko do LC stworzone.**



COMARCH

Katalogi i dziedziczenie



COMARCH

Udostępnianie

Jan Kowalski
GRP_ZARZAD

GRP_ZARZAD
Odczyt: **TAK**,Zapis: **TAK**

Uprawnienia udziału 1

UDOSTEPNIONY KATALOG 1

UDOSTEPNIONY KATALOG 2

Uprawnienia udziału 2

GRP_ZARZAD
Odczyt: **TAK**,Zapis: **NIE**

Uprawnienia NTFS

DANE
GRP_ZARZAD
Odczyt: **TAK**,Zapis: **NIE**

ZARZĄD
GRP_ZARZAD
Odczyt: **TAK**,Zapis: **TAK**

KSIĘGOWOŚĆ
GRP_ZARZAD
Odczyt: **TAK**,Zapis: **NIE**

PRODUKCJA
GRP_ZARZAD
Odczyt: **TAK**,Zapis: **NIE**

IT
GRP_ZARZAD
Odczyt: **TAK**,Zapis: **NIE**

WERSJE INSTALACYJNE

COMARCH

Polecenie - Net Use

Autentykacja = uwierzytelnienie (ang. Authentication) proces polegający na zweryfikowaniu zadeklarowanej tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych.

Autoryzacja (ang. Authorization, także kontrola dostępu, ang. access control) funkcja bezpieczeństwa, która potwierdza, czy dany podmiot jest uprawniony do korzystania z żądanego zasobu.

Łączenie i rozłączanie sesji ze stacji roboczej - polecenie NET USE (wybrane zastosowania)

- Wyświetlenie pomocy: **Net use /?**
- Wyświetlenie listy aktualnych połączeń: **Net use**
- Połączenie do serwera z autentykacją na podanego użytkwonika:
  - **Net use \\nazwa_serwera /user:nazwa_uzytkowika hasło**
- Mapowanie folderu sieciowego na wybraną literę: **Net use z: \\nazwa_serwera\katalog**
- Rozłączenie wszystkich aktualnych połączeń: **Net use /delete ***

COMARCH

Logon skrypt

Jak napisać skrypt:

- Ścieżki w skryptach: gdzie to możliwe KOPIUJEMY, nie wpisujemy [dla uniknięcia literówek]
- Nazwy plików: sugerujące cel skryptu
- Rozszerzenie: .bat – włączenie rozszerzeń znanych typów plików
- Składnia: testujemy z linii komend
  - Przykładowy LOGON skrypt: net use Z: \\szkolenie01\UDZIAL
  - Przykładowy LOGOFF skrypt: net use Z: /delete

Jak zapiąć skrypt:

- Lokalizacja skryptu na dysku:
  - Dla użytkownika: wolumen systemowy -> nazwa domeny -> katalog „scripts”
  - dla GPO: wolumen systemowy -> nazwa domeny -> policies -> GPO -> \User\Scripts -> katalogi logon/logoff
- Podpięcie skryptu:
  - do danego użytkownika/użytkowników – w jego właściwościach
  - do danego OU – przez utworzenie odpowiedniej polityki (GPO)
    - *Group Policy object*/User Configuration/Windows Settings/Scripts (Logon/Logoff)

Weryfikacja:

- Zawsze należy zweryfikować działanie skryptu zanim zaczniemy go używać produkcyjnie

COMARCH

Terminy szkoleń

- Microsoft Windows Server 2008 - kurs podstawowy - PROMOCJA! 1100 PLN zamiast ~~1700 PLN~~

Kraków : 6-9.11.2012 ; Warszawa :16-19.10. 2012

- Microsoft Windows Server 2008 - konfiguracja Active Directory PROMOCJA! 1200 PLN zamiast ~~1900 PLN~~

Kraków: 20-23.11.2012; Warszawa: 18-21.12.2012

Microsoft Windows Server 2008 - konfiguracja infrastruktury sieciowej PROMOCJA! 1200 PLN zamiast ~~1900 PLN~~

Kraków: 3-6.12.2012; Wrocław: 16-19.10.2012

COMARCH