W ćwiczeniu należy wykonać 8 zrzutów ekranu i odpowiedzieć na

dwa pytania z zadania dodatkowego na końcu instrukcji.

Proszę nie kadrować zrzutów, wykadrowany zrzut = brak zrzutu!!!

Zrzuty powinny być czytelne!

Informacja o tym jaki zrzut wykonać, pojawia się w tekście

ćwiczenia, w odpowiednim miejscu, czerwonym drukiem.

Wykonane zrzuty należy umieścić w dowolnym pliku tekstowym z

odpowiednim opisem.

Plik proszę nazwać imię\_nazwisko\_nazwagrupy.\*\*\* i umieścić jako

odpowiedź do zadania.

Zrzuty do wykonania:

WYKONAJ ZRZUT EKRANU DRZEWA KATALOGÓW . (1p)

WYKONAJ ZRZUT EKRANU EKSPLORERA ZE ZMAPOWANYM DYSKIEM. (1p)

WYKONAJ ZRZUT EKRANU Z UPRAWNIENIAMI EFEKTYWNYMI DLA UŻYTKOWNIKA

menedzerTwojeInicjały . (1p)

WYKONAJ ZRZUT EKRANU OKNA KONSOLI GPM Z WIDOKIEM DODANYCH GPO. (1p)

WYKONAJ ZRZUT EKRANU OKNA NETWORK CONNECTIONS Z WŁACZONYMI

OGRANICZENIAMI . (1p)

WYKONAJ 3 DOWOLNE ZRZUTY EKRANU OBRAZUJACE DZIAŁANIE POLIS . (3p)

Odpowiedz :

1. Czym jest spowodowany brak dostępu? (2,5p)

2. Jak zmienić ustawienia karty sieciowej? (2,5p)

Temat 4 – Zarządzanie dostępem do zasobów

Cel tematu

W ramach tematu zdefiniujesz dostęp do folderów i plików zarówno jako lokalny jak i sieciowy.

W ramach tematu nauczysz się:

 Dodawać pliki i foldery

 Przypisywać uprawnienia lokalne do folderów

 Przypisywać uprawnienia sieciowe do folderów

 Przypisywać uprawnienia lokalne do plików

 Definiować ustawienia zaawansowane

 Weryfikować uprawnienia efektywne

Wstęp teoretyczny

Pliki i foldery są podstawowym zasobem dla którego konieczne jest zarządzanie dostępem. Dzięki

kontom i grupom domenowym można poprzez nie przypisywać dostęp do plików i folderów na

różnych komputerach należących do domeny, bez konieczności tworzenia oddzielnych kont na

komputerach użytkowników.

Dostęp może być przypisany:

 Lokalnie – dotyczy użytkowników, którzy korzystają z folderów i plików będąc

zalogowanymi na komputerze, na którym się one znajdują.

 Sieciowo - dotyczy użytkowników, którzy korzystają z folderów i plików będąc

zalogowanymi na innym komputerze, niż na którym się one znajdują, i korzystając z nich

poprzez sieć.

Dla plików i folderów można przypisać uprawnienia:

 Podstawowe, takie jak: odczyt, zapis, usuwanie, modyfikacja czy pełna kontrola

 Zaawansowane jak: przechodzenie przez folder czy uruchomienie aplikacji

Uprawienia domyślnie są dziedziczone. Oznacza to, że jeśli użytkownik ma prawo odczytu plików

w folderze Raporty, to również będzie miał takie prawo w jego pod-folderze Rok2021.

Dziedziczenie można usunąć i w ten sposób zawężać lub poszerzać uprawnienia w folderach.

Definiując uprawnienia należy pamiętać o zasadach:

 Uprawnienia kumulują się – jeśli użytkownik ma do folderu uprawnienie odczytu, a grupa

do której należy, ma do folderu uprawnienia zapisu, użytkownik ma prawo odczytu i

zapisu.

 Wykluczenia mają wyższy priorytet – jeśli użytkownik należy do 5 grup, która mają pełne

uprawnienia do folderu, i do 1, która ma zabroniony odczyt, użytkownik nie będzie miał

prawa odczytu plików (ale zapis tak skoro nie został on mu odebrany).

 Uprawnienia sieciowe są przypisywane jako najbardziej restrykcyjna wersja – jeśli

użytkownik do folderu ma dostęp lokalny ustawiony jako odczyt, a sieciowy jako pełna

kontrola, będzie miał wyłącznie uprawnienia odczytu (część wspólna) – użytkownik nigdy

przez sieć nie może mieć większych uprawnień niż lokalnie.

ZADANIA

Typ zadania: Uprawnienia lokalne plików i folderów

Zadanie 1: Dodaj konto użytkownika o nazwie menedzerAA do jednostki organizacyjnej

Gdansk. Dodaj to konto do grupy menedzerowieGdansk. Jakich innych grup automatycznie to

konto stało się członkiem? Dodaj konto użytkownika o nazwie partnerTwojeInicjały do

kontenera Users.

Na partycji C wirtualnej maszyny serwera utwórz katalog o nazwie Zasoby a w nim podkatalogi o

strukturze zgodnej z rysunkiem poniżej, pamiętając że wybrane foldery powinny mieć przyrostek

Twoich inicjałów a nie DG

Przypisz uprawnienia zgodnie z tabelą poniżej:

Folder Uprawnienia

Zasoby

Wszyscy użytkownicy uwierzytelnieni (czyt. posiadający konto

w domenie) – odczyt i wyświetlenie zawartości

Administratorzy – pełen dostęp (również do wszystkich

podfolderów)

Polska Grupa pracownicyPolska – odczyt i wyświetlenie zawartości

Gdansk Grupa pracownicyGdansk – odczyt i wyświetlenie zawartości

Analitycy Grupa analitycyGdansk – odczyt i wyświetlenie zawartości

AnalitykTwojeInicjały Konto analitykTwojeInicjały – pełen dostęp

Menedzerowie Grupa menedzerowieGdansk – odczyt i wyświetlenie zawartości

MenedzerTwojeInicjały Konto menedzerTwojeInicjały – pełen dostęp

MenedzerAA Konto menedzerAA – pełen dostęp

Gdynia Grupa pracownicyGdynia – odczyt i wyświetlenie zawartości

Analitycy Grupa analitycyGdynia – odczyt i wyświetlenie zawartości

PiotrWolny Konto PiotrWolny – pełen dostęp

Menedzerowie Grupa menedzerowieGdynia – odczyt i wyświetlenie zawartości

PiotrSzybki Konto PiotrSzybki– pełen dostęp

W folderze Zasoby i w każdym z folderów utwórz plik o nazwie dokument.txt, w którym wpisz

nazwę folderu, w którym się on znajduje.

Utwórz w kontenerze Users konto o nazwie partnerTwojeInicjały.

Po kolei przeloguj się na serwerze na konta i wykonaj operacje zgodnie z tabelą poniżej notując

co było możliwe do wykonania a co nie. Wartości w tablicy wskazują jaki powinien być efekt

zgodnie z zadaniem – w przypadku innych rezultatów sprawdź i zmodyfikuj uprawnienia.

konto folder czynność możliwe

wykonanie

partnerTwojeInicjały Zasoby Wejście do folderu Tak

partnerTwojeInicjały Zasoby Odczyt pliku

dokument.txt

Tak

partnerTwojeInicjały Zasoby Usunięcie pliku

dokument.txt

Nie

partnerTwojeInicjały Zasoby/Gdansk Wejście do folderu Nie

analitykTwojeInicjały Zasoby/Gdynia Wejście do folderu Nie

analitykTwojeInicjały Zasoby/Gdansk/Analitycy Wejście do folderu Tak

analitykTwojeInicjały Zasoby/Gdansk/Analitycy Dodanie pliku Nie

analitykTwojeInicjały Zasoby/Gdansk/Analitycy/

AnalitykTwojeInicjały

Wejście do folderu

Tak

analitykTwojeInicjały Zasoby/Gdansk/Analitycy/

AnalitykTwojeInicjały

Dodanie pliku

Tak

menedzerTwojeInicjały Zasoby/Gdansk/Analitycy Wejście do folderu Nie

menedzerTwojeInicjały Zasoby/Gdansk/Menedzerowie Wejście do folderu Tak

menedzerTwojeInicjały Zasoby/Gdansk/Menedzerowie/

MenedzerTwojeInicjaly

Wejście do folderu Tak

menedzerTwojeInicjały Zasoby/Gdansk/Menedzerowie/

MenedzerTwojeInicjaly

Usunięcie pliku

Tak

menedzerTwojeInicjały Zasoby/Gdansk/Menedzerowie/

MenenedzerAA

Wejście do folderu

Nie

Do folderu Zasoby przypisz grupę wbudowaną Wszystkich (Everyone) zabierając jej uprawnienie

Full Control. Kto ma prawo teraz wejść do folderu i co wykonać? Jeśli nie wiesz, sprawdź to

empirycznie.

Sposób wykonania

 Zarządzanie folderami i plikami – Eksplorator windows (File explorer)

 Zmiana uprawnień do pliku lub folderu - operacja Właściwości (Properties) -> zakładka

Uprawnienia (Security)

Szczegółowy tutorial

1. Dodaj konta użytkowników i grup zgodnie z treścią zadania (szczegółowy opis procedury

– temat 3, zadanie 2 i 5)

2. Na maszynie serwera otwórz okno File explorer w lewej dolnej części pulpitu.

3. W oknie File explorer kliknij prawym przyciskiem myszki i wybierz operację New ->

Folder.

4. Jako nazwę folderu podaj Zasoby.

5. Analogicznie dodaj pozostałe foldery zgodnie z treścią zadania.

WYKONAJ ZRZUT EKRANU DRZEWA KATALOGÓW . (1p)

6. Wejdź do folderu Zasoby i dodaj w nim plik tekstowy o nazwie zasoby.txt w którym

wpisz tekst zasoby. Analogiczne czynności zgodnie z treścią zadania wykonaj dla

pozostałych folderów (plik dokument.txt).

7. Wejdź we właściwości (operacja Properties) folderu Zasoby.

8. Przejdź na zakładkę Security. Zgodnie z treścią dostęp: Users (użytkownicy posiadający

konto w domenie) – odczyt; Administratorzy – pełen dostęp.

9. Kliknij na przycisk Edit i postaraj się usunąć występujące tam grupy

Przeczytaj komunikat – dlaczego nie jest to możliwe?

10. Kliknij na przycisk Cancel.

11. Kliknij na przycisk Advanced -> przycisk Disable inheritance. W ten sposób usuniesz

dziedziczenie uprawnień z folderu nadrzędnego, co pozwoli na ich zmianę.

12. Przeczytaj komunikat w oknie dialogowym i wybierz opcję Remove iherited… Spowoduje

to usunięcie odziedziczonych wpisów – ta opcja jest korzystna jeśli chcesz znacząco

zmienić uprawnienia. Jeśli chciałbyś dokonać głownie ich modyfikacji to opcja Convert

inherited… usunęła by dziedziczenie (czyli de facto blokadę zmian) pozostawiając

aktualne uprawnienia.

13. Kliknij OK -> Yes. (przeczytaj uważnie komunikat Windows Security)

14. Ponownie kliknij na przycisk Edit. Lista wpisów jest pusta.

15. Kliknij na przycisk Add.

16. Wpisz Administrator i kliknij na Check names. Pasuje więcej wpisów, więc z listy wybierz

Administrators (udostępnisz folder wszystkim członkom grupy administratorów, a nie

wyłącznie administratorowi głównemu czyli kontu Administrator).

17. Kliknij OK - > OK.

18. Zgodnie z treścią zadania zaznacz na liście uprawnień Full control.

19. Kliknij na przycisk Add.

20. Wpisz auth i kliknij na Check names. Pojawi się Authenticated users.

21. Kliknij OK - > OK.

22. Zgodnie z treścią zadania zaznacz Read oraz List folder contents.

23. Kliknij OK - > OK.

Zdefiniowałeś odpowiednie uprawnienia dla folderu Zasoby

24. Przeloguj się na konto partnerTwojeInicjały. Wykonaj czynności na folderze Zasoby

zgodnie z tabelą zadania. Wykonaj czynności wskazane w tej samej tabeli dla pozostałych

kont.

25. Przeloguj się na konto administratora.

26. Wejdź we właściwości folderu Zasoby.

27. Na zakładce Security przypisz grupę wbudowaną Wszystkich (Everyone) zabierając jej

uprawnienie Full Control (kolumna Deny).

28 Czy możesz wejść do tego folderu? Czy będą mogli wejść do niego inni użytkownicy? – jeśli

tego nie wiesz sprawdź empirycznie.

29. Usuń grupę Everyone z listy uprawnień.

Typ zadania: Udostępnianie i ustawianie uprawnień sieciowych

folderu

Zadanie 2: Udostępnij folder Zasoby pod nazwą Materialy z uprawnieniami udostępnienia

(przez sieć) jako odczytu (read) dla wszystkich użytkowników uwierzytelnionych (Authenticated

users). Połącz się z folderem przez sieć z maszyny klienta jako menedzerTwojeInicjały.

Jakie uprawnienia są lokalne, a jakie zdalne dla konta menedzerTwojeInicjały? Jakie będą

uprawnienia przy dostępie sieciowym jak zmienisz uprawnienia do folderu dla grupy

Authenticated users z odczytu na zmianę (change)?

Dodaj we wpisach udostępnienia folderu sieciowego Materiały grupę analitycyGdansk

zabierając uprawnienie odczytu (Read jako Deny). Połącz się z folderem przez sieć z maszyny

klienta jako analitykTwojeInicjały. Czy jest to możliwe?

Sprawdź listę udostępnionych zasobów na serwerze. Następnie ustaw, aby folder udostępniony

Materialy był ukryty przy przeglądaniu udostępnionych zasobów. Jakie będą uprawnienia przy

dostępie jak zmienisz dostęp do folderu z odczytu na zmianę (change)?

Zdefiniuj dostęp do folderu udostępnionego Materialy jako dysku sieciowego X.

Jak uważasz co należy zrobić aby dostęp do folderu był możliwy dla użytkowników, którzy nie są

zalogowani do domeny? Jeśli nie wiesz spróbuj empirycznie tak skonfigurować folder Zasoby

(wymagane zmiany w ustawieniach uprawnień lokalnych i sieciowych).

Sposób wykonania

 Zarządzanie folderami i plikami – Eksplorator windows (File explorer)

 Udostępnienie folderu - operacja Właściwości (Properties) -> zakładka Udostępnianie

(Sharing)

 Dostęp poprzez sieć do katalogu - \\serwer\zasób, np. \\kontroler.wsb.pl\materialy

 Lista udostępnionych zasobów – konsola Computer Management \ sekcja Shared

Folders

 Ukrycie folderu – na końcu nazwy należy dodać $

 Definiowanie dysku sieciowego – Eksplorator Windows (File explorer) \ menu Narzędzia

(Tools) \ operacja Mapuj dysk sieciowy (Map Network Drive …)

Szczegółowy tutorial

1. Uruchom obie maszyny wirtualne jeśli nie są one uruchomione.

2. Na serwerze wejdź we właściwości folderu Zasoby i przejdź na zakładkę Sharing.

3. Kliknij na przycisk Advanced sharing…

4. Zaznacz pole Share this folder.

5. W pole tekstowe Share name wpisz Materialy.

6. Kliknij na przycisk Permissions.

7. Usuń grupę Everone i dodaj grupę Authenticated users z uprawnieniem Read.

8. Kliknij OK -> OK.

9. Na komputerze klienta zaloguj się jako menedzerTwojeInicjały.

10. Wejdź do folderu sieciowego poprzez przycisk Start -> Uruchom … -> wpisz

\\kontroler.wsb.pl\materialy (tzw. Ścieżka UNC – Universal Naming Convention) i

naciśnij Enter.

11. Wejdź do folderu Polska\Gdansk\Menedzerowie\menedzerTwojeInicjały. Czy jest to

możliwe? Odczytaj plik w dokument.txt. Czy jest to możliwe? Dodaj nowy dokument. Czy

jest to możliwe i czy można było zrobić to lokalnie?

12. Ponownie na serwerze wejdź we właściwości folderu Zasoby i przejdź na zakładkę

Sharing.

13. Kliknij na przycisk Advanced sharing…

14. Kliknij na przycisk Permissions.

15. Dla grupy Authenticated users zaznacz jeszcze uprawnienie Change.

16. Na komputerze klienta będąc dalej zalogowanym jako menedzerTwojeInicjały wejdź

ponownie do folderu sieciowego \\kontroler.wsb.pl\materialy.

17. Wejdź do folderu Polska\Gdansk\Menedzerowie\menedzerTwojeInicjały. Dodaj nowy

dokument. Czy teraz jest to możliwe?

18. Na serwerze wejdź do katalogu

Zasoby\Polska\Gdansk\Menedzerowie\menedzerTwojeInicjały i usuń jego zawartość.

19. Powróć do maszyny klienta. Co stało się z zawartością wyświetlanego folderu?

20. Ponownie na serwerze wejdź we właściwości folderu Zasoby i przejdź na zakładkę

Sharing.

21. Kliknij na przycisk Advanced sharing…

22. Kliknij na przycisk Permissions.

23. Dodaj grupę analitycyGdansk i zaznacz uprawnienie jako Deny.

24. Na komputerze klienta zaloguj się jako analitykTwojeInicjały.

25. Wejdź do folderu sieciowego poprzez przycisk Start -> Uruchom … -> wpisz

\\kontroler.wsb.pl\materialy i naciśnij Enter. Czy jest to możliwe i czy można wejść do

tego folderu lokalnie?

26. Na komputerze klienta zaloguj się jako menedzerTwojeInicjały.

27. Wejdź do folderu sieciowego poprzez przycisk Start -> Uruchom … -> wpisz

\\kontroler.wsb.pl i naciśnij Enter. W ten sposób wyświetliłeś wszystkie katalogi

udostępnione na serwerze.

28. Wejdź do folderu Polska\Gdansk\Menedzerowie\menedzerTwojeInicjały. Czy jest to

możliwe? Odczytaj plik dokument.txt. Czy jest to możliwe? Dodaj nowy dokument. Czy

jest to możliwe i czy można było zrobić to lokalnie?

29. Powróć do maszyny serwera.

30. Naciśnij Windows + Q i wpisz Computer. Z listy wybierz Computer management.

31. Wejdź do sekcji Share folders -> Shares

W tym miejscy widać wszystkie udostępnione udziały, również te ukryte. Oznacza to, że

podając na końcu adres C$ można zobaczyć zawartość całej partycji C.

32. Na komputerze klienta zaloguj się jako menedzerTwojeInicjały.

33. Wejdź do folderu sieciowego poprzez przycisk Start -> Uruchom … -> wpisz

\\kontroler.wsb.pl\C$ i naciśnij Enter. Na szczęście foldery ukryte mają ustawione

uprawnienie dostępu przez sieć tylko dla administratorów.

34. Po pojawieniu się okna podaj login (wsb\administrator) i hasło (zaq1@WSX)

administratora domeny. W ten sposób wyświetliłeś wszystkie katalogi partycji C. Jeśli się

to nie uda przeloguj się na kliencie na administratora.

35. Na serwerze w konsoli Computer manager wejdź do sekcji Share folders -> Shares.

36. Wejdź we właściowości folderu Materialy. Spróbuj zmienić nazwę – niestety nie jest to

możliwe.

37. Usuń udostępnienie poprzez operację Stop sharing.

38. Wybierz klikając prawym przyciskiem myszy operację Start sharing.

39. Kliknij next.

40. Wskaż jako ścieżkę folder C:\Zasoby i przejdź dalej.

41. W share name wpisz Materialy$.

42. Wybierz Administrator have full access; other users have read only access.

43. Finish -> Finish.

44. Na komputerze klienta zaloguj się jako menedzerTwojeInicjały.

45. Wejdź do folderu sieciowego poprzez przycisk Start -> Uruchom … -> wpisz

\\kontroler.wsb.pl\ i naciśnij Enter. Czy zasób Materiały jest widoczny?

46. Zmień adres na \\kontroler.wsb.pl\materialy$ i naciśnij Enter. Czy teraz zasób Materiały

jest widoczny?

47. Na komputerze klienta w Eksplorator Windows (menu Narzędzia główne\ łatwy dostęp)

wybierz operację Mapuj jako dysk

48. Jako dysk wskaż X, a folder \\kontroler.wsb.pl\matarialy$.

49. Sprawdź w eksploratorze plików, że dysk sieciowy się pojawił.

50. Ustaw, aby folder sieciowy Materialy był dostępny dla wszystkich bez konieczności

posiadania konta w domenie (zastosuj grupę Everyone). Sprawdź to logując się do klienta

po koncie lokalnym.

WYKONAJ ZRZUT EKRANU EKSPLORERA ZE ZMAPOWANYM DYSKIEM. (1p)

Typ zadania: Uprawnienia efektywne

Zadanie 3: Użytkownik menedzerTwojeInicjały zgłosił, że nie może utworzyć pliku w

katalogu Zasoby/Gdansk/Menedzerowie w związku z tym, że nie chcesz analizować wszystkich

wpisów aby ustalić jakie rzeczywiście ma on uprawnienia do tego folderu sprawdź uprawnienia

efektywne (czynne).

Sposób wykonania

 Sprawdzanie uprawnień czynnych - właściwości folderu -> zakładka Security ->

ustawienia zaawansowane (przycisk Advanced) \ zakładka Effective Permissions ->

wskazanie grupy/konta, dla którego sprawdzane są uprawnienia efektywne -> przycisk

Select

Szczegółowy tutorial

1. Na maszynie serwera wejdź do właściwości folderu Zasoby/Gdansk/Menedzerowie.

2. Przejdź na zakładkę Security i kliknij na przycisk Advanced.

3. Przejdź na zakładkę Effective permissions.

4. Kliknij w odnośnik Select a user, wskaż konto menedzerTwojeInicjały i zatwierdź

wybór.

5. Kliknij na przycisk View effective access i sprawdź uprawnienia. Czy zgodnie z

wynikami użytkownik powinien móc tworzyć nowe pliki? Jeśli nie to co trzeba

wykonać, aby przyznać mu stosowny dostęp.

WYKONAJ ZRZUT EKRANU Z UPRAWNIENIAMI EFEKTYWNYMI DLA UŻYTKOWNIKA

menedzerTwojeInicjały . (1p)

Temat 5 – Polisy bezpieczeństwa

Cel tematu

W ramach tematu zdefiniujesz szereg ograniczeń jak i usprawnień dla komputerów i

użytkowników w domenie, które zostaną wdrożone w sposób wysoce zautomatyzowany.

Pozwoli to rozwiązać np. poniższy problem administracyjny „W twojej firmie jest około 500

komputerów i tyle samo użytkowników, którymi jako administrator zarządzasz. Chcesz im

wszystkim skonfigurować środowisko pracy. Każdemu użytkownikowi chcesz przekierować folder

Moje Dokumenty na udostępniony dysk sieciowy, oraz zmapować dysk na folder Publiczny.

Chcesz by wszyscy mieli zainstalowaną drukarkę sieciową oraz ograniczony dostęp do Panelu

sterowania. Każdy z użytkowników powinien mieć podobnie wyglądający Pulpit z usuniętymi

niektórymi standardowo dostępnymi elementami oraz stworzonym na nim folderem na

dokumenty prywatne. Do zrealizowania tego zadania skorzystasz z zasad grup (ang. Group

Policy).”

W ramach tematu nauczysz się:

 Delegować uprawnienia

 Tworzyć polisy grupowe

 Ustawiać parametry szczegółowe wdrażania polisy

 Sprawdzać i eksportować ustawienia polisy

 Konfigurować polisę:

o ograniczać interfejs użytkownika i dostępną funkcjonalność

o określać limity dyskowe

o ograniczać dostępne oprogramowanie

o przekierowywać foldery dla poszerzania dostępu do nich

o uruchamiać skrypty startowe

o automatycznie instalować oprogramowanie

o ustawiać bezpieczeństwo: haseł, logowania czy pamięci wirtualnej

o określać preferencje: drukarek czy czynności powiązanych z zamknięciem

pokrywy laptopa

o audytu: monitorowania logowania czy usuwania zasobów

Wstęp teoretyczny

Zasady Grup (ang. Group Policy) w Windows Server mogą być wykorzystane do zarządzania

konfiguracją grup komputerów i użytkowników, poprzez definiowanie opcji związanych z

rejestrami systemu, ustawieniami zabezpieczeń, dystrybucją oprogramowania, skryptów i

przekierowaniem folderów. Dzięki Zasadom Grup można w łatwy sposób zredukować koszty

zarządzania organizacją. Zdefiniowane ustawienia w zasadach grup są przechowywane w GPO (

Group Policy Object), które są tworzone i edytowane przy pomocy narzędzia Group Policy

Management Console (GPMC).

Korzystając z tego narzędzia, linkując GPO do site-u, domeny lub jednostki organizacyjnej, można

przypisać ustawienia do użytkowników i komputerów znajdujących się w danym obiekcie Active

Directory. Jednostka Organizacyjna (OU) jest kontenerem najniższego poziomu w AD, do którego

można przypisać ustawienia Group Policy.

Ustawienia zdefiniowane w GPO, są przechowywane w dwóch lokalizacjach: w Active Directory

w miejscu zwanym kontenerem Group Policy i w folderze Sysvol na kontrolerze domeny gdzie

przechowywane są szablony Group Policy. Kontener Group Policy zawiera atrybuty używane do

rozmieszczania GPO. Informacje przechowywane w szablonach Group Policy zawierają: ustawienia

zabezpieczeń, pliki skryptów, informacje służące do instalacji aplikacji, preferencje i szablony

administracyjne (ang. Administrative template) bazujące na ustawieniach Group Policy.

Szablony administracyjne (pliki z rozszerzeniem \*.ADMX) zawierają ustawienia, które są dostępne

w sekcji Administrative Templates. Szablony administracyjne mogą być przechowywane lokalnie

lub centralnie w folderze Sysvol. Korzystanie z centralnego rozwiązania posiada dwie zalety:

 zawartość folderu Sysvol jest replikowana pomiędzy kontrolerami domeny. GPMC zawsze

używa szablonów administracyjnych przechowywanych centralnie przed lokalna wersją.

Dzięki temu jeden zestaw zaaprobowanych szablonów jest dostępny w całej domenie.

 możliwość korzystania z różnych języków szablonów administracyjnych. Jest to szczególnie

użyteczne dla środowisk rozciągniętych pomiędzy różnymi krajami i używających różnych

języków. Np. jeśli szablony administracyjne są przechowywane w centralnej lokalizacji w

folderze Sysvol, jeden administrator domeny może widzieć ustawienia w języku angielskim

a inny w francuskim.

Kluczową konsolą zarządzania polisami grupowymi jest Group Policy Management. Narzędzie

GPMC udostępnia zunifikowane zarządzanie wszystkimi aspektami zasad grup pomiędzy wieloma

lasami w organizacji. Pozwala zarządzać obiektami GPO, filtrami Windows Management

Instrumentation (WMI) i powiązanymi z group Policy uprawnieniami w sieci. GPMC zawiera zbiór

interfejsów do zarządzania Group Policy opartych o konsolę MMC. Posiada następującą

funkcjonalność:

 Importowanie i eksportowanie GPO

 Kopiowanie i wklejanie GPO

 Tworzenie kopii (backup) i odtwarzanie GPO

 Wyszukiwanie GPO

 Raportowanie

 Group Policy Modeling. Umożliwia symulowanie Resultant Set of Policy (RSoP) do

planowania wdrożenia zasad grup przed ich implementacja w środowisku produkcyjnym

 Group Policy Result. Umożliwia uzyskanie RSoP w celu obserwowania interakcji GPO i

rozwiązywania ewentualnych problemów.

 Wspomaga tworzenie tabel migracji ułatwiających migrację i kopiowanie GPO pomiędzy

domenami i lasami. Tabela migracji jest plikiem mapującym referencje użytkowników,

grup komputerów i ścieżki UNC (Universal Naming Convention w źródłowym GPO na nowe

wartości w GPO docelowym.

 Raporty ustawień GPO i RSoP w postaci HTML które można zapisać i wydrukować

Projektowanie struktury jednostek organizacyjnych wspierającej Group Policy

W środowisku Active Directory przypisujemy ustawienia Group Policy linkując GPO do site-ów,

domen lub jednostek organizacyjnych. Najczęściej większość GPO jest przypisywanych na

poziomie OU, dlatego należy upewnić się, że struktura jednostek organizacyjnych wspiera

strategię zarządzania przy wykorzystaniu Group Policy. Niektóre ustawienia zasad grup np.

dotyczące zasad haseł definiowane są na poziomie domeny. Dobrze zaprojektowana struktura

jednostek organizacyjnych upraszcza administrowanie pozwalając wykorzystać dziedziczenie GPO

i zapobiega duplikowaniu ustawień w różnych GPO.

Projekt struktury jednostek organizacyjnych wymaga balansu pomiędzy wymaganiami

dotyczącymi delegowania praw administracyjnych a potrzebami wynikającymi z korzystania z

Group Policy.

Rekomendacje dotyczące projektowania:

 Delegowanie kontroli administracyjnej– należy tworzyć jednostki organizacyjne w

domenie i delegować administracyjna kontrolę do specyficznych OU dla określonych

użytkowników i grup. Struktura OU będzie efektem wymagań dla delegowania kontroli

administracyjnej.

 Przypisywanie Group Policy – tworząc strukturę OU należy głównie myśleć o obiektach,

którymi chcemy zarządzać. Np. można stworzyć strukturę, której jednostki organizacyjne

definiują stacje robocze, serwery i użytkowników.

Używając struktury gdzie OU zawierają homogeniczne obiekty takie jak użytkownicy lub

komputery (ale nie jedne i drugie jednocześnie), można łatwo wyłączyć te sekcje w GPO, by nie

były aplikowane dla danego typu obiektów.

Przypisywanie Group Policy dla nowego konta użytkownika lub komputera.

Nowe konto użytkownika lub komputera jest domyślnie tworzone odpowiednio w kontenerze

CN=users lub CN= Computers. Nie ma możliwości bezpośredniego przypisania Group Policy do

tych kontenerów oprócz dziedziczenia GPO zlinkowanego z domeną. Redirusr.exe (dla kont

użytkowników) i Redircomp.exe (dla kont komputerów) to dwa narzędzia zawarte w Windows

Server umożliwiające zmianę domyślnej lokalizacji tworzenia kont użytkowników i komputerów,

dzięki czemu można łatwo przypisywać GPO bezpośrednio dla nowo tworzonych obiektów kont.

Narzędzia te są dostępne na serwerze z rolą Active Directory Services Role w folderze

%windir%\system32.

Uruchamiając te narzędzia, raz dla każdej z domen, administrator domeny może wyspecyfikować

jednostkę organizacyjną gdzie będą umieszczane podczas tworzenia nowe konta użytkowników i

komputerów. Umożliwia to administratorom zarządzanie tymi nieprzypisanymi kontami przy

użyciu Group Policy przed umieszczeniem ich w kontenerach docelowych, zwiększając tym samym

bezpieczeństwo tych kont.

Kiedy zmiany w Group Policy są aplikowane?

Zmiany w Group Policy mogą nie być natychmiast dostępne na komputerach użytkowników,

ponieważ zmiana w GPO musi być najpierw replikowana do odpowiedniego kontrolera domeny.

Dodatkowo, klient odświeża Group Policy co 90 minut ( z losowym przesunięciem 30 minut).

Replikacja GPO pomiędzy kontrolerami domen wykorzystuje dwa niezależne mechanizmy:

 Replikacja części przechowywanej w Active Directory jest kontrolowana przez wbudowany

system replikacji AD. Domyślnie trwa to mniej niż minutę pomiędzy kontrolerami w tej

samej lokalizacji. Proces ten może być wolniejszy dla sieci wolniejszych niż LAN.

 Replikacja folderu Sysvol jest kontrolowana przez File Replication Services (FRS) lub

Distributed File System Replication (DFSR). W obrębie lokalizacji (site) FRS replikacja

występuje co 15 minut. Jeśli kontroler domeny jest w innej lokalizacji proces replikacji

zależy od topologii i zdefiniowanych ustawień ( najmniejszy interwał – 15 minut).

Głównym mechanizmem odświeżania Group Policy jest start komputera i proces logowania. Jeśli

jest konieczne, można wyzwolić odświeżenie Group Policy ręcznie, nie czekając na automatyczne

odświeżenie. Aby to zrealizować należy wydać polecenie gpupdate w linii poleceń. Nie można

wyzwolić odświeżenia zasad grup korzystając z narzędzia GPMC.

Definiowanie zasięgu aplikowania Group Policy

Definiując zasięg działania GPO należy wziąć pod uwagę następujące czynniki:

 Gdzie GPO będzie linkowany?

 Jakie filtrowanie zabezpieczeń zostanie użyte?

 Filtrowanie zabezpieczeń (ang. security filtering) umożliwia określenie, którzy użytkownicy

i jakie komputery otrzymają i zastosują ustawienia zdefiniowane w GPO. Dotyczy to całego

GPO i nie może być stosowane do poszczególnych ustawień wewnątrz GPO.

 Jakie filtry WMI zostaną zastosowane?

 Filtry WMI pozwalają dynamicznie określać zasięg GPO bazując na atrybutach docelowego

komputera.

Należy pamiętać, że domyślnie GPO są dziedziczone, kumulowane i mają efekt na wszystkie

komputery i użytkowników w kontenerach Active Direktory i ich dzieciach. Są przetwarzane w

następującej kolejności: Local Group Policy, Site, domena i potem OU, a ostatnio przetwarzane

GPO nadpisuje GPO poprzednie. Domyślne dziedziczenie działa w ten sposób, że najpierw jest

przetwarzane GPO linkowane do kontenera umieszczonego najdalej od obiektu użytkownika lub

komputerem, a GPO linkowane w kontenerach bliższych obiektom nadpisują ustawienia

dziedziczone z GPO wykonywanych wcześniej. Wyjątkiem jest ustawienie opcji Enforced (No

Override) w linku GPO lub Block Policy Inheritance.

Można linkować kilka GPO do jednego kontenera Active Directory, lecz należy być świadomym

priorytetów przetwarzania. GPO z niższym numerem na liście Group Policy Order Link

(wyświetlane na zakładce Linked Group Policy Object w GPMC) jest ważniejsze. Jednak, jeśli jedno

lub więcej linków GPO ma włączona opcję Enforced – najwyżej przypisany link z opcją Enforced

ma pierwszeństwo. Opcja Enforced jest właściwością linku a Block Policy Inheritance jest

właściwością kontenera.

Tworzenie i praca z Group Policy Object

Ponieważ zmiany w GPO są implementowane natychmiast zaleca się, aby GPO było nie linkowane

do czasu przetestowania w środowisku testowym:

 Tworzenie nie linkowanego GPO – w drzewie konsoli GPMC należy kliknąć prawym

przyciskiem myszy w domenie, w której ma być utworzony obiekt i z menu kontekstowego

wybrać polecenie New. W oknie dialogowym New GPO należy podać nazwę i zatwierdzić

przyciskiem OK.

 Edycja GPO - w drzewie konsoli GPMC należy rozwinąćGroup Policy Object, kliknąć prawym

przyciskiem myszy GPO, które ma być edytowane i z menu kontekstowego wybrać

polecenie Edit. W drzewie konsoli należy odnaleźć i zaznaczyćzasady, które mają być

modyfikowane.

 Znaleźć odpowiednie ustawienie w panelu szczegółów i otworzyć jego właściwości

podwójnym kliknięciem. Następnie należy wyedytować ustawienie i nacisnąć przycisk OK.

 Linkowanie GPO – w drzewie konsoli GPMC należy kliknąć prawym przyciskiem myszy

kontener, do którego ma być linkowane GPO i z menu kontekstowego wybrać polecenie

Link an Existing GPO. Inną metodą jest użycie metody drag – and – drop (przeciągnij i

upuść).

 Tworzenie i linkowanie GPO - w drzewie konsoli GPMCnależy kliknąć prawym przyciskiem

myszy kontener, do którego ma być linkowane GPO i z menu kontekstowego wybrać

polecenie Create a GPO in this Domain, and Link it here. W oknie dialogowym New GPO

należy podać nazwę i zatwierdzić przyciskiem OK. W tej procedurze są wykonywane dwie

akcje: jest tworzone GPO w kontenerze Group Policy Object i linkowane do wskazanego

kontenera (np. OU)

 Usuwanie linku do GPO - w drzewie konsoli GPMC należy rozwinąć kontener Group Policy

Object, kliknąć GPO do którego chcemy usunąć link iw panelu szczegółów wybrać zakładkę

Scope. W sekcji Links kliknąć prawym przyciskiem myszy obiekt Active Direktory z linkiem

który chcemy usunąć i z menu poleceń wybrać Delete Link(s). Usuwanie linku różni się od

usuwania GPO. Jeśli kasowany jest tylko link do GPO, GPO nadal istnieje i linki do niego od

innych obiektów AD nadal funkcjonują. Jeśli usuwane jest GPO usuwane są również

wszystkie linki do niego.

 Wyłączanie konfiguracji użytkownika lub komputera w GPO – jeśli tworzone jest GPO z

ustawieniami dotyczącymi tylko użytkowników można wyłączyć ustawienia dotyczące

konfiguracji komputera. Dzięki temu zostanie zredukowany czas startu komputera,

ponieważ ta część nie będzie przetwarzana w celu sprawdzenia czy jakieś ustawienia

istnieją. Jeśli wykorzystane są tylko ustawienia komputera – należy wyłączyć część dla

użytkownika.

 W tym celu w drzewie konsoli GPMC należy rozwinąć kontener Group Policy Object, kliknąć

odpowiednie GPO, w panelu szczegółów wybrać zakładkę Details. W sekcji GPO Status

wybrać pożądane ustawienie: All settings disabled, Computer configuration settings

isabled, Enabled (default), User configuration settings disabled.

ZADANIA

Typ zadania: Delegowanie uprawnień

Zadanie 1: Utwórz konto adminGdansk w jednostce organizacyjnej Gdansk. Deleguj

uprawnienia użytkownikowi adminGdansk dla jednostki organizacyjnej Gdansk dla dodawania,

zarządzania i usuwania grup. Zaloguj się na dodane konto. Dodaj nową grupę o nazwie

programisciGdansk oraz konto użytkownika programistaTwojeInicjały. Czy wszystkie operacje

można było wykonać?

Sposób wykonania

1. Delegacja uprawnień - w konsoli Active Directory Users and Computers, w drzewie konsoli na

odpowiedniej jednostce organizacyjnej, kliknięcie prawym przyciskiem i wybieranie polecenia

Delegate Control -> na stronie Users and Groups dodanie użytkowników i grup ->wskazanie

opcji delegacji.

Szczegółowy tutorial

1. W maszynie serwera w konsoli Active Directory Users and Computers w jednostce

organizacyjnej Gdansk dodaj konto adminGdansk.

2. W maszynie serwera w konsoli Active Directory Users and Computers, zaznacz jednostkę

organizacyjną Gdansk, kliknij prawym przyciskiem i wybierz z sekcji All tasks operacje

Delegate Control.

3. W oknie Delegation of Control Wizard, na stronie Welcome kliknij przycisk Next.

4. Na stronie Users and Groups dodaj użytkownika adminGdansk i kliknij przycisk Next.

5. Na stronie Tasks to Delegate pozostaw opcję Delegate the following common tasks,

zaznacz opcje Create … manage groups (zapoznaj się z innym opcjami) i kliknij przycisk

Next.

6. Na stronie Complete the Delegation of Control Wizard kliknij przycisk Finish.

7. Zaloguj się na konto adminGdansk.

8. W konsoli Active Directory Users and Computers (zaloguj się na konto adminGdansk) w

jednostce organizacyjnej Gdansk dodaj nową grupę o nazwie programisciGdansk oraz

konto użytkownika programistaTwojeInicjały. Czy wszystkie operacje można było

wykonać?

Typ zadania: Szczegółowe ustawianie uprawnień

Zadanie 2: Nadaj użytkownikowi menedzerTwojeInicjały uprawnienia dla jednostki

organizacyjnej Gdansk do resetowania haseł oraz zmiany danych teleadresowych kont

użytkowników. Przeloguj się na konto menedzerTwojeInicjały i zresetuj hasło użytkownikowi

analitykTwojeInicjały oraz zmień mu adres zamieszkania.

Sposób wykonania

 Zarządzanie uprawnieniami obiektów - konsola Active Directory Users and Computers

 Ustawienie dostępu do trybu zaawansowanego – menu View -> opcja Advanced

Features

 Ustawianie uprawnień szczegółowych - właściwości jednostki organizacyjnej -> zakładka

Security / Sekcja Zaawansowane (przycisk Advanced) -> dodanie wpisu (przycisk Add):

o Wskazanie użytkownika

o Wskazanie obiektu – pole listy Apply onto

o Określenie uprawnień: operacji (zakładka Object), właściwości (zakładka

Properties)

Szczegółowy tutorial

1. Zaloguj się jako administrator.

2. W maszynie serwera w konsoli Active Directory Users and Computers w menu View

wybranie opcji Advanced Features. Zauważ, że pojawiły się w konsoli nowe sekcje i

operacje.

3. Zaznacz jednostkę organizacyjną Gdansk, i wejdź w jej właściwości (operacja Properties).

4. Przejdź na zakładkę Security.

5. Kliknij na przycisk Advanced.

6. Kliknij Add

7. Kliknij na odnośnik Select a principal.

8. Dodaj użytkownika menedzerTwojeInicjały (przycisk Advanced -> Find now). Zatwierdź

OK.

9. Rozwiń listę Applies to i zobacz jakie są ustawienia. Domyślnie zaznaczona opcja This

object and all descendant objects oznacza, że wskazane uprawnienia będą mieć

zastosowanie dla jednostki organizacyjnej dla której są one definiowane, jak i jednostek

które się w niej znajdują, itd. Wybierz Descendant user objects (obiekty kont

użytkowników).

10. W sekcji Permissions (uprawnienia w zakresie wykonywania czynności) zaznacz opcje

Reset password.

11. W sekcji Properties (uprawnienia w zakresie zmiany informacji o obiekcie typu adres)

zaznacz Write private information oraz Write phone and mail options.

12. Zaloguj się na konto menedzerTwojeinicjały (CRTL + ESC -> dla wskazanego konta w

prawym górnym rogu operacja Sing out).

13. W konsoli Active Directory Users and Computers (zaloguj się na konto

menedzerTwojeInicjały) w jednostce organizacyjnej Gdansk zresetuj hasło dla

analitykTwojeInicjały oraz zmień mu adres zamieszkania (operacja Properties ->

zakładka Address oraz General). Czy wszystkie operacje można było wykonać?

Typ zadania: Tworzenie polis grupowych

Zadanie 3: Utwórz 2 polisy grupowe o nazwach: Firma oraz OddzialGdansk. Pierwszą przypisz

całej domenie wsb.pl a drugą jednostce organizacyjnej Gdansk. Zablokuj dziedziczenie a następnie

je wymuś. Jak wpływa to na kolejność implementacji polis?

Sposób wykonania

 Zarządzanie polisami - konsola Group Policy Management -> kontener z nazwą domeny.

 Utworzenie obiektu polisy - w kontenerze Group Policy Objects operacja New

 Przypisanie obiektu polisy – na domenie lub jednostce organizacyjnej wskazanie operacji

Link an Existing GPO... i wybranie z listy wcześniej utworzonej polisy

 Utworzenie i przypisanie polisy - polisę można jednocześnie utworzyć i przypisać do

domeny/jednostki organizacyjnej poprzez operację Create a GPO in this domain, and Link

it here….

 Blokowanie dziedziczenia - dla jednostki organizacyjnej zaznaczenie opcji Block

Inheritance

 Wymuszenie dziedziczenia – dla linku do polisy operacja Enforced

 Sprawdzenie kolejności implementacji polis - dla jednostki organizacyjnej we

właściwościach polisy należy przejście na zakładkę Group Policy Inheritance

Szczegółowy tutorial

1. W maszynie wirtualnej serwera przejdź do konsoli Server Manager -> menu Tools ->

konsola Group Policy Management (GPM).

2. W konsoli GPM przejdź do sekcji Group Policy Objects dla domeny wsb.pl.

3. Na sekcji Group Policy Objects wybierz operację New i jako nazwę podaj Firma. Dodaj

kolejną polisę o nazwie OddzialGdansk.

4. Na domenie wsb.pl wybierz operację Link an Existing GPO... i wskaż z listy polisę Firma.

5. Na jednostce organizacyjnej Gdansk wybierz operację Link an Existing GPO... i wskaż z

listy polisę OddzialGdansk.

6. Dla zaznaczonej jednostki Gdansk sprawdź zakładki:

a. Linked Grouped Policy Object – polisy bezpośrednio przypisane

b. Group Policy Inheritance – wszystkie polisy wpływające na jednostkę (polisy

bezpośrednio przypisane + polisy dziedziczone z kontenerów, w których

jednostka bezpośrednio/pośrednio się znajduje). Ile jest przypisanych polis i jaka

jest ich kolejność wdrażania? Co to oznacza?

7. Na jednostce organizacyjnej Gdansk wybierz operacje Block Inheritance. Ile polis jest

wdrażanych dla jednostki?

8. Usuń blokowanie dziedziczenia dla jednostki organizacyjnej Gdansk (operacja Block

Inheritance)

9. Na domenie wsb.pl dla podłączonej poniżej polisy Firma (link) wybierz operację

Enforced.

10. Dla zaznaczonej jednostki Gdansk na zakładce Group Policy Inharitance sprawdź

przypisane polisy. Jak zmieniła się ich kolejność?

WYKONAJ ZRZUT EKRANU OKNA KONSOLI GPM Z WIDOKIEM DODANYCH GPO. (1p)

Typ zadania: Ustawianie parametrów szczegółowych polisy

Zadanie 4: Sprawdź jakie szczegółowe ustawienia polisy mogą być określane. Spowoduj, aby

polisa OdzialGdansk była wdrażana dla wszystkich pracowników z Gdańska (pracownicyGdansk)

oprócz menedżerów (menedzerowieGdansk). Jakie można zastosować w tym celu rozwiązania,

które jest najlepsze?

Sposób wykonania

 Zarządzanie polisami - konsola Group Policy Management

 Właściwości polisy - zakładki:

o Scope – określenie kont użytkowników i grup, dla których polisa ma być

wdrażana

o Delails – określenie wdrażanych obszarów polisy (komputera i użytkownika)

o Delegation – lista wykluczeń poprzez zablokowanie odczytu polisy

Szczegółowy tutorial

1. W maszynie wirtualnej serwera przejdź do konsoli Server Manager -> menu Tools ->

konsola Group Policy Management (GPM).

2. W konsoli GPM przejdź do domeny wsb.pl -> jednostka organizacyjna Polska/Gdansk.

3. Zaznacz link do polisy o nazwie OddzialGdansk.

TA POLISA JEST WDRAŻANA DLA WSZYSTKICH KONT KOMPUTERÓW I

UŻYTKOWNIKÓW, KTÓRE SIĘ ZNAJDUJĄ W JEDNOSTCE ORGANIZACYJNEJ GDANSK. DLA

INNYCH JEDNOSTEK ORGANIZACYJNYCH JAK NP. GDYNIA JUŻ NIE.

4. Na zakładce Scope sprawdź sekcję Security Filtering. Wskazuje one dla kogo polisa

będzie mieć zastosowanie (domyślnie Authenticated Users, czyli wszyscy użytkownicy

uwierzytelnieni). Zmieniając w tym miejscu uprawnienia dla kogo polisa ma być

wdrażana. Należy wziąć pod uwagę jednak, że zmieniając ustawienia w tym miejscy

zmieniane są one dla polisy, a jeśli będzie ona podczepiona (podlinkowana) w wielu

miejscach, we wszystkich zostaną zaimplementowane zmiany.

5. Przejdź na zakładkę Details i przejrzyj informację o utworzeniu polisy. Rozwiń listę i

sprawdź jakie są możliwości określenia jej implementacji:

a. Enabled (domyślnie) – polisa jest włączona

b. All settings disabled – polisa jest wyłączona (czyt. jej ustawienia nie są wdrażane)

c. Computer configuration / User configuration settings disabled – wyłączenie

działania sekcji komputera (dla kont komputerów, np. pobieranie czasu z

serwera) lub użytkownika (dla kont użytkowników, np. wyświetlanie panelu

sterowania). Każda polisa ma takie 2 sekcje.

6. Przejdź na zakładkę Delegation. Pozwala ona definiować listę wykluczeń poprzez

zablokowanie odczytu polisy poszczególnym grupom i użytkownikom. Jak myślisz jaki jest

tego cel?

7. Przejdź na zakładkę Scope i sekcji Security Filtering. Dodaj grupę pracownicyGdansk.

W TEN SPOSÓB POLISA BĘDZIE MIEĆ ZASTOSOWANIE TYLKO DLA KONT UŻYTKOWNIKÓW

ZNAJDUJĄCYCH SIĘ W JEDNOSTCE ORGANIZACYJNEJ GDANSK I NALEŻĄCYCH DO GRUPY

PRACOWNICYGDANSK.

Czy dla grupy menedzerowieGdansk będzie mieć ona również zastosowanie?

8. Przejdź na zakładkę Delegation. Dodaj grupę menedzerowieGdansk, pozostawiając w

polu Permissions ustawienie domyślne.

9. Mając zaznaczoną grupę menedzerowieGdansk kliknij na przycisk Advanced. Dla grupy

menedzerowieGdansk zaznacz dla uprawnienia Read (odczyt polisy) opcję Deny.

W ten sposób spowodowałeś, że polisa nie będzie odczytywana przez konta

użytkowników (czyli użytkowników) należących do grupy menedzerowieGdansk, a zatem

dla nich implementowana.

10. Działanie ustawień dostępu przetestujesz w kolejnym zadaniu.

Typ zadania: Konfigurowanie polisy – ograniczanie interfejsu

użytkownika

Zadanie 5: Przenieś konto komputera Klient do jednostki organizacyjnej Gdansk. Dla dodanej

polisy przypisanej do jednostki organizacyjnej Gdansk ustaw szereg ograniczeń:

 Usuń menu run

 Zablokuj dostęp do rejestru

 Wyłącz automatyczne odtwarzanie w napędzie CD/DVD

 Zablokuj możliwości zmiany pulpitu

 Zmodyfikuj działanie Internet Explorera - wyświetlanie wyłącznie zakładek General i

Security

 Ogranicz możliwości zmiany sieci:

o zmiany ustawień TCP / IP

o Włączania / wyłączania połączeń

o Sprawdzania aktualnych połączeń

 Na koniec zablokuj dostęp do całego panelu sterowania.

 Wymuś wdrożenie ustawień dla polis w maszynie serwera i klienta.

Na komputerze klienta zaloguj się kolejno na konta: PiotrSzybki, menedzerTwojeInicjały,

analitykTwojeInicjały. Będąc zalogowanym na każdym z kont kolejno sprawdź dostępność i

działanie: menu run, rejestr, pulpit, Internet Exporer, ustawienia sieci, panel sterowania notując,

które z kont może korzystać z których funkcjonalności? Określ, które ustawienia polis na to

wpływają.

Sposób wykonania

 Zarządzanie polisami - konsola Group Policy Management

 Definiowanie polisy - na nazwie polisy operacja Edit – nastąpi pojawienie się konsoli

Group Policy Management Editor (Group Policy Object Editor w Server 2003 i starszych)

 Wymuszenie odświeżenia (wdrożenia) polisy – polecenie gpupdate / force

Szczegółowy tutorial

1. Uruchom obie maszyny wirtualne jeśli nie są one uruchomione.

2. W maszynie wirtualnej serwera przejdź do konsoli Server Manager -> menu Tools ->

konsola Active Directory Users and Computers.

3. W sekcji Computers zaznacz konto Klient i wybierz operację Move.

4. Wskaż jako nową lokalizację jednostkę organizacyjną Gdansk.

W ten sposób dla komputera Klient zastosowana będzie polisa o nazwie OddzialGdansk,

przypisana dla jednostki organizacyjnej Gdansk.

5. W maszynie wirtualnej serwera przejdź do konsoli Server Manager -> menu Tools ->

konsola Group Policy Management (GPM).

6. W konsoli GPM przejdź do domeny wsb.pl -> jednostka organizacyjna Polska/Gdansk.

7. Zaznacz link do polisy o nazwie OddzialGdansk i wybierz operację Edit.

8. Pojawi się konsola Group Policy Management Editor.

W związku z tym, że możliwości konfigurowania działania komputerów muszą być szerokie

spektrum polisy posiadają dziesiątki tysięcy ustawień, których poznanie wymaga zaangażowania

znacznego czasu (5-cio dniowe szkolenie).

Sekcja Computer Configuration – ustawienia tej sekcji będą implementowane dla wszystkich kont

komputerów, które znajdują się w jednostce organizacyjnej / domenie do której przypisana jest

polisa. Np. jeśli wyłączony zostanie panel sterowania, a w jednostce organizacyjnej ma konto

komputer o nazwie MK-Komputer, to niezależnie kto (czyt. jakie będzie konto użytkownika)

„usiądzie” przy komputerze nie będzie mieć dostępu do panelu sterowania.

Sekcja User Configuration – ustawienia tej sekcji będą implementowane dla wszystkich kont

użytkowników, które znajdują się w jednostce organizacyjnej / domenie do której przypisana jest

polisa. Np. jeśli wyłączony zostanie panel sterowania, a w jednostce organizacyjnej ma konto

użytkownika o nazwie DariuszGryzio, to niezależnie na którym komputerze się on zaloguje nie

będzie mieć dostępu do panelu sterowania. Polisa zatem „podąża” za kontem użytkownika.

9. Rozwiń sekcje User Configuration \ Policies \ Administrative Templates \ Start Menu

and Taskbar.

10. 10. Posortuj dla łatwiejszego znalezienia listę ustawień klikając na nagłówek kolumny

Settings.

11. Zaznacz opcję Remove Run …

Przeczytaj opis po lewej stronie, stanowi on ważną, szybko dostępną dokumentację.

12. Dla zaznaczonego ustawienia wybierz operację Edit a w oknie zaznacz pole Enabled.

Wyłączyłeś usunięcie menu Run – a dokładnie włączyłeś usunięcie menu run (uruchom).

13. Analogicznie zdefiniuj pozostałe ustawienia korzystając z poniższych danych:

a. Rejestr - User Configuration \ Policies \ Administrative Templates \ System \ Prevent

access to registry … (włącz również opcję … running Silently – co ona oznacza?)

b. Autoplay - User Configuration \ Policies \ Administrative Templates \ Windows

Components \ AutoPlay Policies \ Turn off …

c. Pulpit - User Configuration \ Policies \ Administrative Templates \ Desktop \ Prohibit

adjusting …; User Configuration \ Policies \ Administrative Templates \ Desktop \

Desktop:

Poprzez Desktop Wallpaper ustaw konkretną tapetę.

d. Panel sterowania - User Configuration \ Policies \ Administrative Templates \ Control

Panel \ Prohibit access to control …

e. Internet Explorer:

a. Computer Configuration \ Policies \ Administrative Templates \ Windows

Components \ Internet Explorer \ Internet Control Page :

b. User Configuration \ Policies \ Administrative Templates \ Windows

Components \ Internet Explorer:

f. TCP/IP - User Configuration \ Policies \ Administrative Templates \ Network \

Network Connections

WYKONAJ ZRZUT EKRANU OKNA NETWORK CONNECTIONS Z WŁACZONYMI

OGRANICZENIAMI . (1p)

14. Wymuś wdrożenie polis (standardowo ma to miejsce raz na 180 minut czy po

zrestartowaniu komputera). Wymuś ich wdrożenie wchodząc do konsoli Command

Prompt (Wiersz Polecenia) lub PowerShell (na serwerze) i wprowadzając polecenie

gpupdate / force.

Czynność tą wykonaj będąc na koncie administratora zarówno na maszynie serwera, jak i

klienta. Zastosuj się do wskazówek konsoli, np. że wymagane jest zrestartowanie komputera.

15. Zrestartuj maszynę klienta.

16. Na komputerze klienta zaloguj się kolejno na konta: PiotrSzybki, menedzerTwojeInicjały,

analitykTwojeInicjały. Będąc zalogowanym na każdym z kont kolejno sprawdź

dostępność i działanie: menu run, rejestr, pulpit, Internet Explorer, ustawienia sieci,

panel sterowania notując, które z kont może korzystać z których funkcjonalności.

WYKONAJ 3 DOWOLNE ZRZUTY EKRANU OBRAZUJACE DZIAŁANIE POLIS . (3p)

Zadanie dodatkowe

Zaloguj się na serwer na konto administratora. Wejdź w ustawienia sieci i wybierz opcję

Change adapter options.

Pojawi się komunikat:

Odpowiedz :

3. Czym jest to spowodowane? (2,5p)

4. Jak zmienić ustawienia karty sieciowej? (2,5p)