Politechnika Białostocka

Wydział Elektryczny

Katedra Telekomunikacji i Aparatury Elektronicznej

Instrukcja do zajęć laboratoryjnych

Temat ćwiczenia:

Stosowanie zasad grup (GPO) w usłudze Active Directory

Numer ćwiczenia: 8

Laboratorium z przedmiotu:
Zarządzanie sieciami teleinformatycznymi 2

Kod przedmiotu: TS1A611 254

Białystok 2018

1. Stosowanie zasad grup GPO w usłudze AD

1.1. Wprowadzenie do koncepcji zasad grup

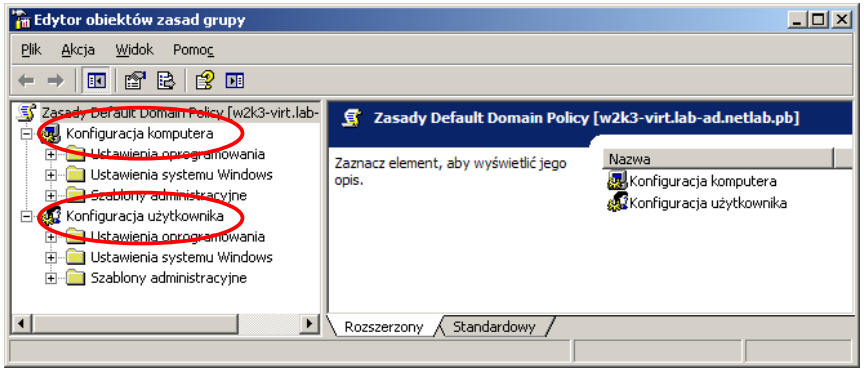
W usłudze Active Directory zasady grup GPO (*Group Policy Objects*) pozwalają na automatycznego zarządzanie i konfigurowania dużej liczby komputerów klienckich czy serwerów. Pozwalają one na zdefiniowanie różnych grupowych ustawień i opcji dla wielu użytkowników i komputerów pracujących pod kontrolą systemu Windows Server.

Zasady grup są zbiorami ustawień kontrolującymi zachowanie zarówno stacji klienckich jak i serwerów pod bardzo wieloma aspektami. Umożliwiają głęboką ingerencję w zachowanie systemów Windows. Pozwalają między innymi na kontrolę pulpitów użytkowników pod wieloma aspektami. Dostępnych opcji są setki, a niektóre z nich to na przykład blokowanie dostępu do panelu sterowania, ograniczenie funkcji menu start, ukrycie ikony *Mój komputer,* zablokowanie uruchamiania określonego programu itd. Za pomocą GPO możemy ponadto kontrolować zachowanie komputerów klienckich czy serwerów. Mamy do dyspozycji szereg ustawień, których przykładem mogą być:

- konfiguracja uprawnień do folderów;
- konfiguracja rejestru;
- instalacja i zarządzanie aplikacjami;
- definiowanie skryptów;
- przekierowanie folderów;
- konfiguracja IE.

Konkretne ustawienia w ramach zasady grup tworzą tzw. obiekt zasad grup (*Group Policy Object* – GPO). Każdy taki obiekt składa się z dwóch części :

- ustawień użytkownika – ustawienia w tej części dotyczą kont osób logujących się w sieci;
- ustawień komputera – pozwalają wymuszać określone parametry w odniesieniu do konkretnych maszyn.



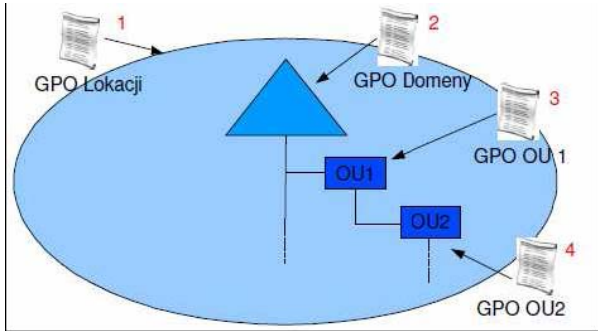
Rys. 1.1. Widok zasady GPO w edytorze zasad grup

Dzięki temu możliwe jest na przykład określenie, że użytkownik *Student,* niezależnie od komputera na którym się loguje, ma mieć zablokowaną możliwość zmiany hasła. Z drugiej natomiast strony możemy chcieć, aby każdy, kto zaloguje się na jednym konkretnym komputerze, nie mógł uruchomić *Windows Installer'a* – wtedy opcję tą konfigurujemy w węźle ustawień komputera.

Obiekty GPO mogą być przypisywane w Active Directory w kilku miejscach:
- lokalnie;
- na poziomie lokacji;
- domeny;
- jednostki organizacyjnej.

Lokalne GPO przechowywane jest, jak nazwa wskazuje, na każdym pojedynczym komputerze osobna. Dotyczy więc ono ustawień tylko tej jednej maszyny. Ten typ GPO jest używany najczęściej w środowisku sieciowym, w którym nie istnieje Active Directory. GPO lokalne umożliwia kontrolę zachowania systemu, ale wymaga ręcznej konfiguracji na każdym komputerze z osobna. Ten rodzaj GPO jest więc mało efektywny w większych sieciach, w których to stosuje się nielokalne obiekty zasad grup. To właśnie takie GPO są wykorzystywane przez Active Directory. Ponieważ zasady PGO mogą być przypisywane na różnych poziomach, istotne jest określenie kolejności ich stosowania. Najczęściej obiekty GPO są aplikowane w następującej kolejności :
- GPO lokalny;
- GPO lokacji;
- GPO domeny;
- GPO jednostek organizacyjnych.

Jest to ustawienie domyślne, jednak istnieje także możliwość wpływania na kolejność stosowania zasad GPO. Zgodnie z powyższą kolejnością, ustawienia zawarte w lokalnym GPO mogą być zastąpione przez GPO lokacji, te z kolei przez GPO domeny itd. (rysunek 3.2).



Rys. 1.2. Kolejność stosowania zasad GPO

Ustawienia zawarte w obiektach GPO są domyślnie dziedziczone. Oznacza to, iż skonfigurowanie jakiejś opcji w GPO przypisanym na poziomie domeny włączy ją we wszystkich jednostkach organizacyjnych tej domeny. Dzieje się tak oczywiście tylko wtedy, gdy któraś z polis (zasad) aplikowanych później nie zmienia tego ustawienia na inne. Załóżmy, że skonfigurowaliśmy w polisie domenowej *opcję A* jako włączoną. Jeżeli w polisie jednostki organizacyjnej opcja ta będzie miała stan *włączony* lub *nieskonfigurowany*, w efekcie końcowym pozostanie włączona. Jeżeli natomiast opcja ta będzie wyłączona na poziomie OU, w efekcie końcowym także pozostanie wyłączona. Powyżej opisany mechanizm możemy modyfikować na dwa sposoby : blokując dziedziczenie i konfigurując *brak zastępowania*. Włączenie pierwszej opcji powoduje zignorowanie ustawień w polisach przypisanych do wszystkich kontenerów nadrzędnych. Wyjątkiem są tylko GPO z atrybutem *nie zastępuj*. W tym przypadku blokada dziedziczenia nie działa. Widać więc, że opcja *No override* (*nie zastępuj)* ma niejako większy priorytet. Należałoby jeszcze wspomnieć o mechanizmie *pętli zwrotnej*. Jest to specjalny tryb przetwarzania polisy polegający na tym, że ustawienia są stosowane niezależnie od tego, czy dany obiekt leży w jednostce organizacyjnej do której polisa jest przypisana czy nie. Jest to użyteczne w sytuacji, gdy przykładowo mamy jednostkę *Biuro* z kontami użytkowników oraz jednostkę *Servers* z serwerami, do której to podłączona została polisa. Serwery te są krytyczne, więc chcemy, niezależnie od tego kto się na nie loguje, wymusić pewne ustawienia. W tym przypadku skonfigurowanie takiej polisy w trybie *pętli zwrotnej* spowoduje, ze każdy użytkownik, niezależnie gdzie znajduje się jego konto w Active Directory, po zalogowaniu na serwer z jednostki *Servers* będzie miał zaaplikowane ustawienia takiej polisy. Działanie mechanizmów dziedziczenia oraz jego blokowania zostało pokazane w jednej z prezentacji wideo dołączonych do publikacji.

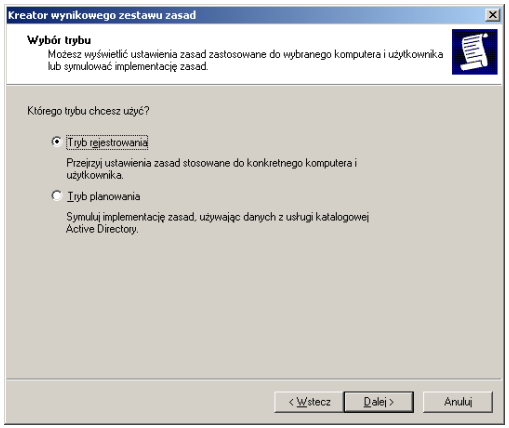
1.2. Narzędzia do konfiguracji GPO

Do zarządzania zasadami (tzw. polisami) GPO system Windows udostępnia kilka narzędzi.

1) *Edytor obiektów zasad grup.* Stanowi on podstawowe narzędzie konfigurowania zasad GPO. Jest to przystawka do konsoli mmc, która udostępnia interfejs pozwalający na edycję konkretnych GPO. Wszystkie opcje możliwe do skonfigurowania w polisie są pogrupowane w odpowiedni sposób. Najbardziej ogólnym podziałem jest wyodrębnienie części konfiguracji użytkownika i komputera. Następnie w ramach każdej z tych gałęzi widoczne są dalsze kontenery. Poprzez wybór pozycji edytorze mamy możliwość zmiany ustawień poszczególnych opcji w danym GPO. Do edytora możemy dostać się na kilka sposobów : dodając odpowiednią przystawkę w konsoli mmc, otwierając go z poziomu *Użytkownicy i komputery usługi Active Directory* lub korzystając z przystawki GPMC (o której trochę więcej poniżej). Edytor GPO pozwala ponadto na aplikowanie ustawień *szablonów zabezpieczeń* oraz *szablonów administracyjnych.* Szczególnie ta druga opcja, umożliwiająca dodawanie własnych opcji do edytora GPO tworzy z GPO bardzo potężne narzędzie kontroli systemów Windows.

2) RSOP (*Resultant Set of Policy, Wynikowy zestaw zasad)* jest także przystawką konsoli mmc. Służy ona do diagnozowania problemów z GPO. RSOP może pracować w jednym z dwóch trybów:
   - **logowania** – służącym do rozwiązywania problemów z już istniejącymi polisami;
   - **planowania** – służącym do planowania i przewidywania zachowań GPO przed wdrożeniem w środowisku produkcyjnym.

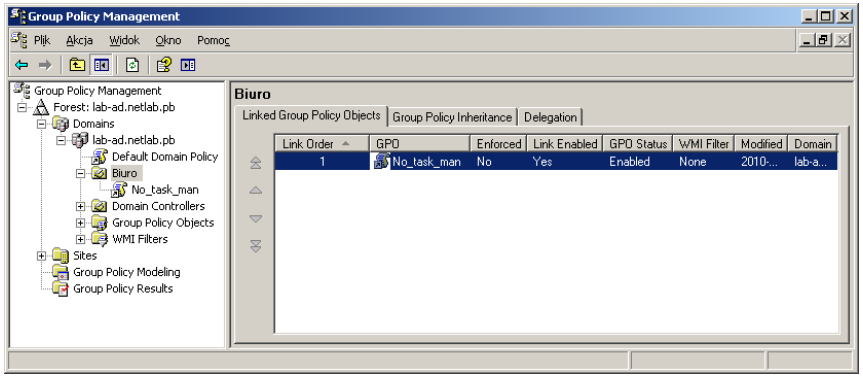
W sytuacji gdy jakieś ustawienia nie są aplikowane, lub są stosowane niezgodnie z naszymi oczekiwaniami, przystawka RSOP jest idealnym narzędziem do sprawdzenia które polisy są obowiązujące, które zostały odrzucone, jakie są efektywne ustawienia obowiązujące danego użytkownika czy komputer itd. (rysunek 3.3).



Rys. 1.3. Tryby pracy narzędzia RSOP.

3) Narzędzia wiersza poleceń : *gpresult, gpupdate.* Pierwsze z nich pełni funkcję podobną do RSOP – pozwala z wiersza poleceń wyświetlić obowiązujące w danej chwili polisy. Gpupdate natomiast umożliwia natychmiastowe odświeżenie ustawień. Jest to przydatne w szczególności wówczas, gdy testujemy pewne ustawienia i nie chcemy czekać przez kilkadziesiąt minut aż komputer sam odświeży listy GPO. Korzystając z polecenia gpupdate możemy natychmiast wymusić aktualizację wszystkich ustawień GPO.

4) Przystawka GPMC (*Group Policy Management Konsole)* – to chyba najbardziej kompleksowe narzędzie do kontroli działania GPO. Z poziomu tej przystawki możliwe jest zarówno uruchamianie edytora GPO w celu zmiany ustawień, jak i podłączanie polis do określonych miejsc (domena, jednostki organizacyjne), możliwość wyłączenia części danej polisy (np. obowiązywać mają tylko ustawienia użytkownika), zablokowanie dziedziczenia, czy nawet wygenerowanie danych RSOP. Jest to narzędzie integrujące poprzednio omawiane konsole w jedno spójne centrum zarządzania GPO. Konsola ta (rysunek 3.4) nie jest instalowana domyślnie, ale można ją bezpłatnie pobrać ze stron firmy Microsoft.



Rys. 1.4. Widok ekranu konsoli GPMC.

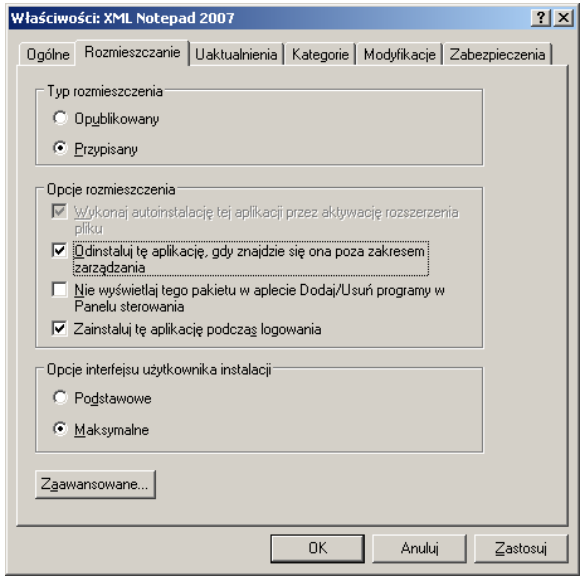
1.3. Ograniczanie zakresu obowiązywania GPO

Obiekty GPO nie są przypisywane do użytkowników czy grup, a do lokacji, domen czy jednostek organizacyjnych. Pozornie może wydawać się, że GPO są przypisywane do grup. Jednak w rzeczywistości obiekty GPO mogą być jedynie filtrowane w oparciu o członkowstwo w grupach, ale do grup jako takich przypisywane być nie mogą. Aby dana polisa mogła zostać zastosowana, użytkownik lub komputer musi posiadać prawo *odczytu* oraz *zastosowania* danej polisy. Cofając więc te prawa możemy łatwo wykluczyć pewną grupę spod obowiązywania danego GPO. Drugim sposobem ograniczania zasięgu GPO jest filtrowanie za pomocą skryptów WMI (*Windows Management Instrumentation)*. Przykładowo możliwe jest skonfigurowanie polisy, która będzie skojarzona ze skryptem WMI wybierającym tylko komputery z wyłączonym firewallem. W polisie takiej możemy następnie skonfigurować dosyć restrykcyjne ustawienia działania systemu (ze względu na wyłączony firewall).

1.4. Instalowanie oprogramowania za pomocą GPO

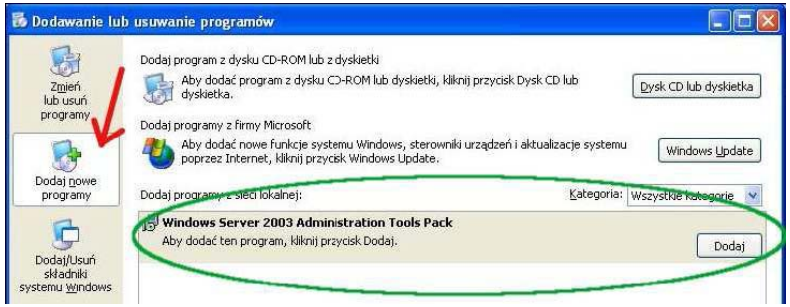
Mechanizm GPO pozwala na instalację oprogramowania. Ta funkcjonalność ograniczona jest niestety tylko do programów dostarczonych w postaci paczek .msi lub plików .zap, ale istnieją darmowe narzędzia pozwalające takie właśnie pliki tworzyć z dowolnych innych rodzajów instalatorów.

Zanim przystąpimy do wdrożenia instalacji musimy zastanowić się, w jaki sposób oprogramowanie to ma być rozdystrybuowane. Po pierwsze, czy dany program ma być instalowany na określonych komputerach (niezależnie od tego, kto na nich pracuje), czy tylko podczas logowania określonej grupy użytkowników. Odpowiedź na to pytanie determinuje, czy opcje instalacji konfigurować powinniśmy w części ustawień komputera czy użytkownika. Kolejną kwestią nad którą musimy się zastanowić, to czy oprogramowanie ma być instalowane podczas logowania obowiązkowo, czy też użytkownik będzie miał możliwość instalacji na żądanie. GPO pozwala bowiem programy *publikować (publish) lub przypisywać (assign)* – rysunek 3.5.



Rys. 1.5. Ustawienia instalacji oprogramowania poprzez GPO.

W pierwszym przypadku efekt działania GPO będzie taki, że użytkownikowi po uruchomieniu z panelu sterowania opcji *Dodaj, usuń programy* pojawi się do wyboru opcja instalacji opublikowanej aplikacji (rysunek 3.6).

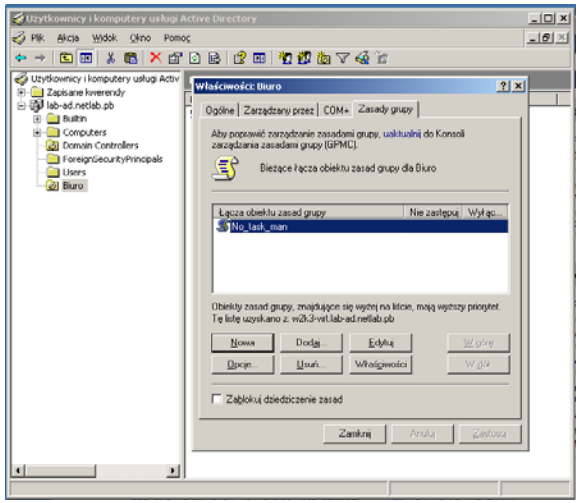


Rys. 1.6. Instalacja oprogramowania opublikowanego przez GPO.

Natomiast w momencie użycia opcji *przypisz* dany program zostanie automatycznie zainstalowany podczas logowania użytkownika bez jego interwencji. Pozostało nam już tylko zdecydowanie, czy chcemy aby w momencie wyłączenia danego GPO oprogramowanie zostało odinstalowane czy nie. Zazwyczaj zaleca się włączanie takiej konfiguracji, ponieważ jeżeli nie wymusimy odinstalowania, tracimy możliwość późniejszego automatycznego usunięcia danego programu. Zmusza nas to do ręcznej rekonfiguracji stacji klienckich których dotyczyło GPO.

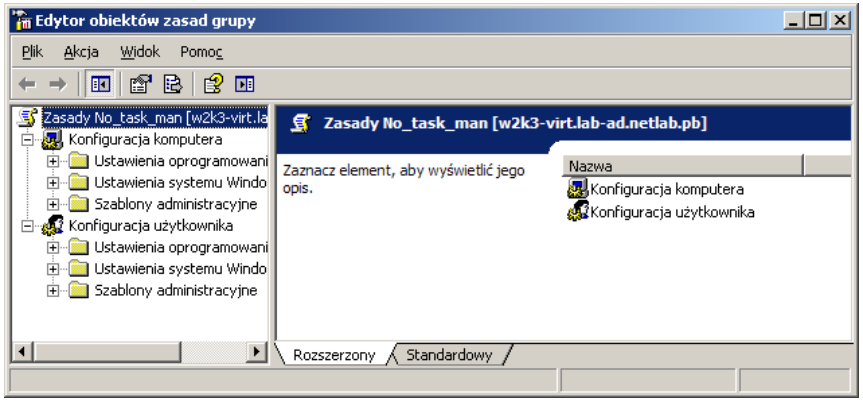
1.5. Przykład definiowania i wdrażania zasady GPO

Jako przykład przedstawione będzie utworzenie zasady GPO blokującej dostęp do *Menedżera zadań* dla użytkowników znajdujących się w jednostce organizacyjnej *Biuro*. W tym celu w przystawce *Użytkownicy i komputery usługi Active Directory* wybieramy naszą domenę, tworzymy w niej nową jednostkę organizacyjną *Biuro* następnie jej Właściwości i zakładkę *Zasady* grupy (rysunek 3.7).



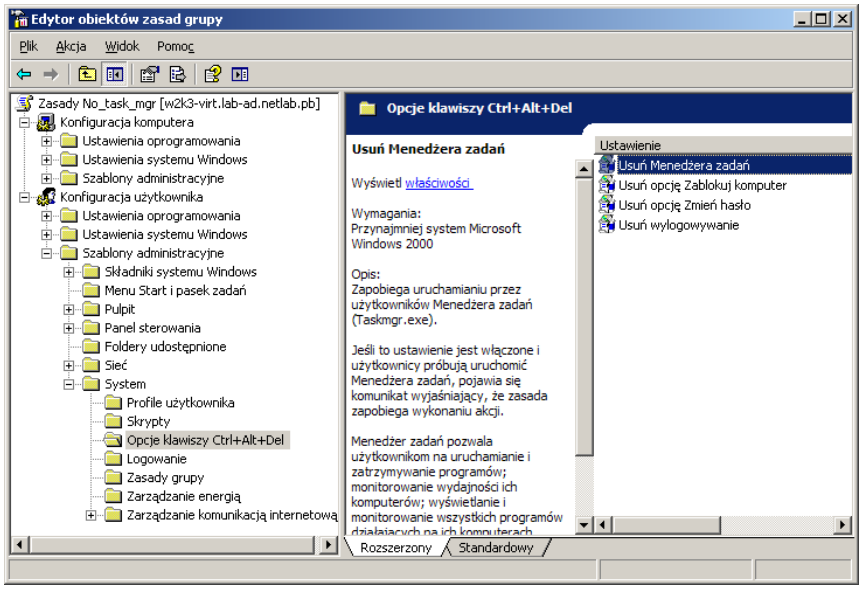
Rys. 1.7. Zakładka *Zasady grupy* we właściwościach jednostki organizacyjnej *Biuro*.

Następnie tworzymy nową zasadę *No_task_man* i przechodzimy do jej edycji (rysunek 3.8).



Rys. 1.8. Edycja zasady *No_task_man*.

W grupie *Konfiguracja użytkownika* wybieramy *Szablony administracyjne -> System -> Opcje klawiszy Ctrl+Alt+Del* i włączamy ustawienie *Usuń Menedżera zadań* (rysunek 3.9).



Rys. 1.9. Umiejscowienie ustawienia *Usuń Menedżera zadań* w zasadzie *No_task_man.*

Aby sprawdzić działanie utworzonej zasady, należy w jednostce organizacyjnej *Biuro* utworzyć nowego użytkownika lub przenieść tam istniejącego użytkownika domenowego. Po zalogowaniu się na konto tego użytkownika opcja menedżer zadań powinna być nieaktywna (rysunek 3.10).

Rys. 1.10. Efekt zastosowania zasady *No_task_man.*

1.6. Plan wykonania ćwiczenia

1. Utworzyć przedstawioną w punkcie 1.5 zasadę blokującą dostęp do *Menedżera zadań* i sprawdzić jej działanie.
2. Zdefiniować zasadę grupy ustawiającą dla użytkowników z jednostki organizacyjnej *Biuro* określoną tapetę na pulpicie.
3. Zdefiniować zasadę grupy blokującą dla użytkowników z jednostki organizacyjnej *Biuro* dostęp do ustawień ekranu.
4. Utworzyć zasadę grupy ustawiającą dla użytkowników z jednostki organizacyjnej *Biuro* określoną stronę startową w przeglądarce Internet Explorer. Użytkownicy nie powinni mieć możliwości zmiany tak wdrożonego ustawienia strony głównej.
5. Skonfigurować zasadę grupy automatycznie instalującą dla użytkowników z jednostki organizacyjnej *Biuro* oprogramowanie edytora XML (plik XmlNotepad.msi).

Sprawozdanie

W sprawozdaniu należy przedstawić wykonaną konfigurację oraz zamieścić opis przeprowadzonych prób mających na celu potwierdzenie zgodności działania utworzonego systemu z wstępnymi założeniami.

Wymagania BHP

Zgodnie z podanymi na pierwszych zajęciach i potwierdzonymi przez studentów zasadami obowiązującymi w pomieszczeniu, w którym odbywają się ćwiczenia. Stosowny regulamin BHP jest też wywieszony w pomieszczeniu laboratorium.

Literatura

1. S. Reimer, M. Mulcare: Active Directory dla Microsoft Windows Server 2003. Przewodnik techniczny. APN Promise, Warszawa, 2005.
2. S. Gotojuch, E. Nowacka: Microsoft Windows Server 2003: projektowanie i organizacja Active Directory oraz usług zabezpieczeń. APN Promise, 2005.
3. J. Spealman, K. Hudson, M. Kraft, A. Steven: Planowanie, wdrażanie I obsługa infrastruktury Active Direktory Windows Server 2003. Training Kit 70-294. Wydanie II. APN Promise, Warszawa, 2007.