**Ćwiczenie 6: 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:
	+ ograniczać interfejs użytkownika i dostępną funkcjonalność
	+ określać limity dyskowe
	+ ograniczać dostępne oprogramowanie
	+ przekierowywać foldery dla poszerzania dostępu do nich
	+ uruchamiać skrypty startowe
	+ automatycznie instalować oprogramowanie
	+ ustawiać bezpieczeństwo: haseł, logowania czy pamięci wirtualnej
	+ określać preferencje: drukarek czy czynności powiązanych z zamknięciem pokrywy laptopa
	+ 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 2008 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 (Rys. 1). 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 rozwinąć Group Policy Object, kliknąć prawym przyciskiem myszy GPO, które ma być edytowane i z menu kontekstowego wybrać polecenie Edit. W drzewie konsoli należy odnaleźć i zaznaczyć zasady, 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

**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. 7. Zaloguj się na konto adminGdansk (CRTL + ESC -> dla wskazanego konta w prawym górnym rogu operacja Sing out).
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?

**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):
	+ Wskazanie użytkownika
	+ Wskazanie obiektu – pole listy Apply onto
	+ Określenie uprawnień: operacji (zakładka Object), właściwości (zakładka Properties)

**Szczegółowy tutorial:**

1. 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.
2. Zaznacz jednostkę organizacyjną Gdansk, i wejdź w jej właściwości (operacja Properties).
3. Przejdź na zakładkę Security.
4. Kliknij na przycisk Advanced.
5. Kliknij na odnośnik Select a principal.
6. Dodaj użytkownika menedzerTwojeInicjały (przycisk Advanced -> Find now). Zatwierdź OK.
7. 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).
8. W sekcji Permissions (uprawnienia w zakresie wykonywania czynności) zaznacz opcje Reset password.
9. W sekcji Properties (uprawnienia w zakresie zmiany informacji o obiekcie typu adres) zaznacz Write Street Address oraz Write Telephone Number.
10. Zaloguj się na konto menedzerTwojeinicjały (CRTL + ESC -> dla wskazanego konta w prawym górnym rogu operacja Sing out).
11. 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?

**Zadanie 3**: Utwórz 2 polisy grupowe o nazwach: Firma oraz OddzialGdansk. Pierwszą przypisz całej domenie zsl.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 zsl.pl.
3. Na sekcji Group Policy Objects wybierz operację New i jako nazwę podaj Firma. Dodaj kolejną polisę o nazwie OddzialGdansk.
4. Na domenie zsl.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?

1. Na jednostce organizacyjnej Gdansk wybierz operacje Block Inheritance. Ile polis jest wdrażanych dla jednostki?
2. Usuń blokowanie dziedziczenia dla jednostki organizacyjnej Gdansk (operacja Block Inheritance)
3. Na domenie zsl.pl dla podłączonej poniżej polisy Firma (link) wybierz operację Enforced.
4. Dla zaznaczonej jednostki Gdansk na zakładce Group Policy Inharitance sprawdź przypisane polisy. Jak zmieniła się ich kolejność?

**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:
	+ Scope – określenie kont użytkowników i grup, dla których polisa ma być wdrażana
	+ Delails – określenie wdrażanych obszarów polisy (komputera i użytkownika)
	+ 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 zsl.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.

1. 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.
2. 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.

1. Przejdź na zakładkę Delegation. Pozwala ona definiować listę wykluczeń poprzez zablokowanie odczytu polisy poszczególnym grupom i użytkownikom. Jak myślisz jaki jest tego cel?
2. 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?

1. Przejdź na zakładkę Delegation. Dodaj grupę menedzerowieGdansk, pozostawiając w polu Permissions ustawienie domyślne.
2. 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.
3. Działanie ustawień dostępu przetestujesz w kolejnym zadaniu.

**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: janKowalski, 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
* Lokalizacje kluczowych ustawień:
	+ Menu start - User Configuration \ (Policies w 2008 i 2012 Server) \ Administrative Templates \ Start Menu and Taskbar \ Remove Run …
	+ Rejestr - User Configuration \ Administrative Templates \ System
	+ Autoplay – User Configuration \ Administrative Templates \ Windows Components \ AutoPlay Policies
	+ Pulpit - User Configuration \ Administrative Templates \ Desktop
	+ Internet Explorer :
		- Computer Configuration \ (Policies w 2008 i 2012 Server) \ Administrative Templates \ Windows Components \ Internet Explorer
		- User Configuration \ Administrative Templates \ Windows Components \ Internet Explorer
	+ TCP/IP - User Configuration \ Administrative Templates \ Network \ Network Connections
	+ Panel sterowania - User Configuration \ Administrative Templates \ Control Panel
* 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 zsl.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 michalKuciapski, to niezależnie na którym komputerze się on zaloguje nie będzie mieć dostępu do panelu sterowania. Polisa zatem „podąża” za kontem użytkownika.

1. Rozwiń sekcje User Configuration \ Policies \ Administrative Templates \ Start Menu and Taskbar.
2. Posortuj dla łatwiejszego znalezienia listę ustawień klikając na nagłówek kolumny Settings.
3. Zaznacz opcję Remove Run Menu from Start Menu
Przeczytaj opis po lewej stronie, stanowi on ważną, szybko dostępną dokumentację.
4. Dla zaznaczonego ustawienia wybierz operację Edit a w oknie zaznacz pole Enabled.
Wyłączyłeś usunięcie menu Run – a dokładnie włączyłeś usunięcie menu run (uruchom).
5. 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:
Jeśli wystarczy czasu poprzez Desktop Wallpaper ustaw konkretną tapetę.

d. Panel sterowania - User Configuration \ Policies \ Administrative Templates \ Control Panel \ Prohibit access to control …

e. Internet Explorer

Computer Configuration \ Policies \ Administrative Templates \ Windows Components \ Internet Explorer \ Internet Control Page

User Configuration \ Policies \ Administrative Templates \ Windows Components \ Internet Explorer:
f. TCP/IP - User Configuration \ Policies \ Administrative Templates \ Network \ Network Connections

1. 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.
2. Zrestartuj maszynę klienta.
3. Na komputerze klienta (XP) zaloguj się kolejno na konta: janKowalski, 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.
4. Określ, które ustawienia polis na to wpływają?