ActiveDirectory – konta, grupy, zasady grupy.

1. Wstęp teoretyczny.

Active Directory to Microsoft'owa implementacja protokołu sieciowego warstwy aplikacji **LDAP** (ang. Lightweight Directory Access Protocol). Protokół LDAP stosowany jest w tak zwanych **usługach katalogowych**. Usługa katalogowa to nic innego jak **obszerna**, **hierarchiczna baza danych**, zawierająca informacje o **użytkownikach**, **grupach użytkowników**, **komputerach**, a także **zasobach sieciowych**, działających w sieciach firmowych, gdzie pracują serwery Microsoft'owe. To nic innego jak zbiór informacji o użytkownikach sieci, ich uprawnieniach do różnego rodzaju zasobów, komputerach, na jakich pracują, konfiguracji tych komputerów i tak dalej. Active Directory pozwala administratorom sieci, centralnie, z poziomu jednego komputera (odpowiednio skonfigurowanego serwera) zarządzać całym zbiorem użytkowników w sieci, określać ich uprawnienia do zasobów sieciowych, a także konfigurować komputery, na których pracują. To potężne narzędzie zdecydowania ułatwia pracę administratora w sieciach, gdzie pracują dziesiątki użytkowników i komputerów. Na całość usług związanych z Active Directory składa się aż **pięć elementów**:

a. **AD Domain Services.**
b. AD Certificate Services.
c. AD Lightweight Directory Services.
d. AD Rights Management Services.
e. AD Federation Services.

Pojęcia związane z Active Directory:

a. **Magazyn danych -** plik, przechowywany na dysku serwera, zawierający informacje o obiektach usługi katalogowej. Obiektem usługi katalogowej może być użytkownik, grupa, jednostka organizacyjna czy też komputer. Plik nosi nazwę NTDS.dit.
b. **Kontroler domeny -** serwer, na którym zainstalowano **Active Directory**, przechowujący kopię magazyny danych. Wyróżnić możemy kontrolery typu **Global Catalog** (katalog globalny), a także kontrolery tylko do odczytu - **Read-Only Domain Controler** oraz odczytu i zapisu – **Writeable Domain Controler**.
c. **Domena** – obszar sieci, któremu przydzielono określone możliwości oraz zasoby. W niej skupione są **obiekty Active Directory**, takie jak użytkownicy, grupy, jednostki organizacyjne oraz komputery działające w jej obrębie. Aby można było domenę utworzyć, wymagany jest przynajmniej **jeden kontroler**.
d. **Las -** zbiór jednej lub też wielu domen. Pierwsza domena, która zostanie utworzona w lesie, będzie tak zwaną domeną główną lasu, a cały las przyjmie nazwę taką jak domena główna. Jeśli przykładowo tworzymy nową domenę w nowym lesie i nazwiemy ją ***test.local*** to **cały las przyjmie taką nazwę**.
e. **Drzewo -** jedna domena, albo kilka domen pracujących pod tą samą **przestrzenią nazw DNS**.
f. **Jednostka organizacyjna** – to obiekt usługi AD, pozwalający na przechowywanie użytkowników, grup użytkowników oraz komputery. Jednostkom organizacyjnym można przypisywać poszczególne **zasady grupy** oraz **delegować uprawnienia administracyjne**.

szkola.local pracownia1.szkola.local

Wymagania systemów klienckich korzystających z Active Directory:

Każdy komputer kliencki, z zainstalowanym systemem Windows (7, 8.1 oraz 10) może pracować w domenie pod dwoma warunkami:

a. musi być w wersji przynajmniej **Professional** (może być w wersji **Ultimate** lub **Enterprise**), żadnej z wersji **Home** do domeny **nie podłączymy**,
b. oprócz licencji na sam system, do każdego klienta należy dokupić **dodatkową licencję** pozwalającą na korzystanie z zasobów serwera. Licencja to nosi nazwę **CAL (ang. Client Access License)**.

Implementacja usług katalogowych Active Directory na serwerach polega na zainstalowaniu odpowiedniej usługi. Usługa nazywa się **Usługi Domenowe Active Directory** *(Active Directory Domain Services)*. Jeśli to pierwsza nasza domena w lesie, to oprócz instalacji samej usługi, musimy jeszcze promować nasz serwer do roli kontrolera domeny.

Zasady Grupy (ang. **Group Policy**) to **zbiór reguł i ustawień** określających zakres działania komputera oraz użytkowników danego komputera. Są to ustawienia definiujące do jakich elementów systemu, takich jak na przykład **panel sterowania**, użytkownik komputera ma dostęp, a do jakich nie. **Z jakich aplikacji** może korzystać, a z jakich nie może, a także czy może instalować i usuwać **urządzenia peryferyjnie** i korzystać z **dysków przenośnych**. Zbiór reguł, które możemy zdefiniować jest ogromny, do dyspozycji mamy grubo ponad **2000** różnego rodzaju ustawień i konfiguracji. Zasady grupy są nieodłącznym elementem **usługi Active Directory** i wraz z nią dają największe możliwości. Korzystając z Zasad Grupy za pośrednictwem Active Directory konfigurujemy je na serwerze i decydujemy dla jakich komputerów oraz użytkowników mają zostać wdrożone. Wszystkie ustawienia przechowywane są w tak zwanych **Obiektach Zasad Grupy** (ang. **Group Policy Object**).

Istnieją również **zasady lokalne**, które można skonfigurować na **każdym komputerze z systemem Windows**, nawet jeśli nie należy do domeny, wówczas jednak nie mamy możliwości ich wdrażania zdalnego, a co więcej ilość opcji konfiguracyjnych jest znacznie mniejsza. Lokalny edytor zasad grupy uruchomić można wybierając ***START*** i wprowadzając polecenie ***gpedit.msc***

Edytor zasad na serwerze, dostępny będzie po wpisaniu polecenia ***gpmc.msc*** w oknie uruchamiania programu (***klawisz Windows + R***). Można go również uruchomić wybierając:

a. dla **Windows Server 2012 R2:** ***Menadżer Serwera -> Narzędzia (Tools) -> Edytor Obiektów Zasad Grupy (Group Policy Managment)***
b. dla **Windows Server 2008 R2:** ***START -> Narzędzia Administracyjne (Administrative Tools) -> Edytor Obiektów Zasad Grupy***

Wyobraźmy sobie sytuacje, że **dla całej domeny** (a właściwie użytkowników tej domeny) **zabroniliśmy dostępu do panelu sterowania**. **Konkretnej jednostce organizacyjnej** z kolei, **zezwoliliśmy na obsługę panelu**. Jak zatem będzie przedstawiała się kwestia dostępu dla użytkowników należących do tej jednostki organizacyjnej? **Otóż będą oni mogli korzystać z panelu** – dlaczego? Dlatego, że w p**ierwszej kolejności przetwarzane są zasady przypisywane dla jednostek organizacyjnych** i to one mają pierwszeństwo. Nawet jeśli zabronimy czegoś dla całej domeny, a zezwolimy dla jednostki to te ustawienia będą miały **priorytet**. Kolejność przetwarzania zasad przedstawia poniższy diagram:

Kolejna ważna kwestia to **wdrażanie zasad**. Po tym jak dokonamy modyfikacji w obiektach zasad powinna nastąpić ich **aktualizacja**, zarówno na **serwerze**, jak również na **kliencie**. Zasady aktualizowane są **automatycznie**, co pewien czas, jednak po każdej modyfikacji obiektów warto wykonać taką **aktualizację ręcznie**. Służy do tego polecenie ***gpupdate /force*** wprowadzane w konsoli systemowej. Polecenie wykonać można na serwerze oraz na kliencie. Wówczas mamy pewność, że wszystkie zamiany, których dokonaliśmy zostaną wprowadzone od razu. Jeśli chodzi o samych klientów to aktualizacja zasad odbywa się **również podczas ponownego logowania** do systemu oraz po upływie określonego czasu. Czas ten wynosi między **90**, a **120 minut**.

2. Zakres laboratorium:

W ramach laboratorium student ma za zadanie zaimplementować na wirtualnym obrazie Windows Server usługę ActiveDirectory. Po udanej implementacji usługi należy dokonać konfiguracji i zarządzania obiektami w ActiveDirectory. Polega to na dodaniu nowych użytkowników i połączeniu ich z odpowiednimi grupami, oraz ewentualnym przypisaniu zasad dla poszczególnych użytkowników lub grup użytkowników.

Przykładowe zastosowanie takiego mechanizmu to aktualnie działająca domena, z której studenci korzystają podczas zajęć na pracowniach komputerowych w budynku B5. Istnieje domena główna do której logują się studenci. Każdy student posiada swoje konto i określone zasady pracy. Administrator może zdalnie lub lokalnie poprzez domenę zarządzać wszystkimi komputerami i użytkownikami podpiętymi do domeny. Ewentualna zmiana na domenie odnośnie komputera klienckiego w łatwy sposób może zostać zrealizowana na wszystkich komputerach (np.: doinstalowanie nowego softu).

3. Przebieg laboratorium:

Uruchamiamy komputery logując się na swoje domenowe konta Windows 10. Po zalogowaniu uruchamiamy program VirtualBox, z menu wybieramy *Maszyna -> Dodaj* i wskazujemy na obraz Windows Server 2012 R2 znajdujący się na dysku lokalnym C:\ w katalogu Vms, analogicznie postępujemy aby uruchomić drugi obraz z Windows 10. Uruchamiamy obydwie maszyny, na Windows 10 logujemy się danymi: **login – *root*, hasło – *l4b_w1nd0ws***, na Windows Server: **login – *Administrator*, hasło – *l4b_s3rw3r.***

Uwaga !! aby zalogować się na maszynie z Windows Server należy najpierw wcisnąć Ctr + Alt + Delete, nie zawsze działa jak należy, aby ta konfiguracja zadziałała na maszynie należy z menu z widokiem maszyny wybrać Wejście -> klawiatura -> naciśnij ctrl + alt + delete !!

a. Instalacja usługi ActiveDirectory (Windows Server 2012 R2):
   - Po zalogowaniu i załadowaniu system przystępujemy do pracy
   - Uruchamiamy ***Menadżer Serwera*** (***Server Manager) z menu Start (jeżeli nie uruchomi się sam)***
   - Klikamy ***Dodaj Role i Funkcje (Add Roles and Features)***
   - Zostawiamy domyślne zaznaczenie i klikamy ***Dalej (Next)*** trzy razy
   - W zakładce ***Role serwera*** (**Server Roles)** wybieramy i zaznaczamy w pustym kwadraciku ***Usługi domenowe Active Directory***, klikamy w nowym oknie które wyskoczy ***Dodaj funkcje*** (***Add Features)*** i po chwili ***Dalej (Next)***
   - W zakładce ***Funkcje*** (**Features)** klikamy ***Dalej (Next)***
   - W zakładce ***Usługi AD DS*** klikamy ***Dalej (Next)***
   - W zakładce ***Potwierdzenie*** (***Confirmation***) klikamy ***Instaluj (Install)*** i czekamy ~ 1 min
   - **Po zakończeniu procesu instalacji nie klikamy *Zakończ* (*Close)* !!** w oknie pośrodku klikamy w podświetlony na błękitno link ***'podnieś poziom tego serwera do poziomu kontrolera domeny' (Promote this Server to a domain controller)*** – opcja pojawi się poprawnym dokończeniu instalacji
   - Zaznaczamy ***dodaj nowy las (Add new forest)*** i wprowadzamy nazwę np.: szkola.local (nazwa domeny) i klikamy ***Dalej (Next)***
   - W zakładce ***opcje kontrolera domeny*** (***Domain Controller***) wprowadzamy hasło (0-9, aA) do odzyskiwania w polu ***hasło,*** klikamy ***Dalej (Next)***
   - W kolejnych zakładkach ***DNS, Opcje Dodatkowe, Ścieżki i przegląd opcji (DNS, Additional Options, Paths, Review)*** klikamy ***Dalej (Next)*** – czekamy chwilkę po każdym wyborze
   - Czekamy chwilkę aż serwer zbierze wszystkie informacje (zakładka ***wymagania wstępne Prerequisites***), klikamy ***Instaluj (Install)*** i czekamy
   - Po procesie instalacji klikamy ***Zakończ (Close)*** i restartujemy serwer (serwer powinien sam to zrobić, jeżeli nie robimy to ręcznie)
   - Po restarcie logujemy się na konto (dane bez zmian) – mamy utworzoną domenę, zainstalowaną usługę ActiveDirectory, możemy teraz poprzez ***Menadżer Serwera (Server Manager)*** zarządzać domeną, komputerami do niej podpiętymi oraz użytkownikami do niej zalogowanymi (klikamy w prawym górnym rogu ***Narzędzia*** (***Tools)*** i wybieramy ***Użytkownicy i komputery Active Directory (ActiveDirectory Users and Computers)***

Następnym krokiem jest zmiana adresu IP serwera w celu utworzenia jednej wspólnej sieci domenowej do której będą podłączeni klienci.

b. Zmiana adresu IP serwera:
   - Klikamy ***start –> panel sterowania -> sieć i Internet -> centrum sieci i udostępniania -> zmień ustawienia karty sieciowej -> PPM na połączeniu ETH -> właściwości***
   - Zaznaczamy ***protokół internetowy w wersji 4 (tcp/ipv4) -> właściwości***
   - Zmieniamy adres IP serwera IPv4 na adres statyczny ***10.0.0.1, maska: 255.255.255.0,*** w polu brama domyślna (**Gateway)** nie wpisujemy nic, **DNS zaznaczamy statyczne: 10.0.0.1 (takie samo jak IP serwera !!)**
   - Zatwierdzamy zmiany

c. Wyłączamy zaporę sieciową na Serwerze:
    - Klikamy ***start -> panel sterowania -> system i zabezpieczenia -> zapora systemu Windows -> z lewej strony włącz lub wyłącz zaporę Windows***
    - Wyłączamy zaporę w trzech miejscach: dla sieci prywatnej, publicznej i domenowej, zatwierdzamy zmiany

Wyłącznie całkowite zapory zarówno na Windows Server jak i innych Windowsach nie jest wskazane !! Jednakże dla potrzeb realizacji laboratorium aby uniknąć dodatkowej konfiguracji zapory i wyjątków w zaporze zaleca się wyłączyć całkowicie zapory. Aby uniknąć sytuacji stresującej należy stosować wszelkie środki ostrożności i zabezpieczyć zarówno serwer jak i komputer osobisty. Można już dodawać komputery do domeny, przełączamy się na okno w Windows 10 (maszyna wirtualna !!). Jeżeli nie jesteśmy zalogowani to logujemy się na dane podane na początku tego punktu.

d. Zmiana adresu IP klienta, oraz wyłączenie zapory Windows:
    - Zmieniamy interfejs sieciowy klienta na interfejs połączony z serwerem
    - Klikamy ***start -> wyszukujemy panel sterowania -> sieć i Internet -> centrum sieci i udostępniania -> zmień ustawienia karty sieciowej -> PPM na połączenie ETH -> właściwości***
    - Zaznaczamy ***protokół internetowy w wersji 4 (tcp/ipv4) -> właściwości***
    - Ustawiamy **statyczny adres IP: 10.0.0.2 (10.0.0.1 to adres serwera !!), maska 255.255.255.0, Gateway: 10.0.0.1 (czyli adres serwera !!), pole DNS: 10.0.0.1 (IP serwera ponieważ to on udostępnia usługę DNS !!)**
    - Wyłączamy zaporę systemową
    - Klikamy ***start -> wyszukujemy panel sterownia -> system i zabezpieczenia -> zapora Windows Defender -> z lewej strony włącz lub wyłącz zaporę Windows, wybieramy dwa razy wyłącz: dla sieci prywatnej i publicznej, zatwierdzamy zmiany***
    - Uruchamiamy konsolę cmd: ***start -> w polu wyszukiwania wpisujemy cmd -> Enter*** , w konsoli wpisujemy ***ping 10.0.0.1*** (czyli adres serwera, sprawdzamy czy jest on widoczny, ping musi wyjść pozytywny !!, jeżeli ping jest negatywny znaczy że adresacja jest błędna, czasami należy zresetować obrazy zarówno Win Server jak i Win 10 na maszynie wirtualnej)

e. Dodanie komputera do domeny (Windows 10)
    - Klikamy ***start -> wyszukujemy panel sterowania -> System i zabezpieczenia -> system***
    - Z prawej strony klikamy ***zmień ustawienia***
    - Wybieramy zakładkę ***Nazwa Komputera -> Identyfikator sieciowy*** i na trzech kolejnych oknach klikamy **Dalej** bez żadnych zmian !!
    - W oknie ***wpisz nazwę (…) podajemy login i hasło administratora serwera (dane z logowania do Windows Serwer), oraz nazwę domeny: SZKOLA.LOCAL*** (wybrana podczas instalacji ActiveDirectory), klikamy **Dalej**
    - Nazwę komputera wprowadzamy jako: **STACJA1**, domena komputera: **SZKOLA.LOCAL**, klikamy **Dalej**
    - Wprowadzamy jeszcze raz login, hasło i nazwę domeny ***(dane z logowania do Windows Serwer), oraz nazwę domeny: SZKOLA.LOCAL*** (wybrana podczas instalacji ActiveDirectory),, klikamy *OK*
    - Resetujemy wirtualną maszynę z **Windows 10**

Na maszynie Windows Serwer **w *Menadżer Serwera*** (**Server Manager) w *Użytkownicy i komputery Active Directory*** w zakładce ***Komputery*** powinna pojawić się pozycja Stacja1. Jest on już przypisany do domeny. Pora na użytkowników komputera, którzy będą mogli korzystać z komputera przypisanego do domeny.

f. Nowy użytkownik komputera należącego do domeny (Windows Serwer):
   - W ***Server Manager*** wybieramy z górnego rogu ***Narzędzia*** i klikamy w *Użytkownicy i komputery Active Directory*
   - Z lewej strony nowego okna rozwijamy pozycję szkola.local (domena)
   - Na nazwie domeny klikamy ***PPM -> nowy -> użytkownik***
   - Uzupełniamy dane nowego użytkownika, login i hasło (swoje dane), klikamy *Dalej*
   - Zaznaczamy ***hasło nigdy nie wygasa***, potwierdzamy i mamy już użytkownika komputera pracującego w domenie

g. Zarządzanie (Windows Serwer):
   - Dodanie jednostek organizacyjnych: ***Menadżer Serwera*** (***Server Manager) -> Użytkownicy i komputery Active Directory,*** klikamy PPM na nazwie domeny i wybieramy ***nowy -> jednostka organizacyjna***, wprowadzamy nazwę np.: *uczniowie*, *nauczyciele, administracja.*
   - Dodanie grupy: klikamy PPM na nazwie domeny i wybieramy ***nowy -> grupa***, nadajemy jej nazwę np.: *klasa1*, zasięg zostawiamy jako *Globalny*, typ zabezpieczenia *Security*, klikamy *OK*.
   - Dodanie użytkownika: klikamy PPM na nazwie domeny i wybieramy ***nowy -> użytkownik*** i wprowadzamy dane odnośnie nowego użytkownika (główne to login i hasło, nazwa logowania do domeny). Na użytkowniku klikamy PPM i wybieramy ***dodaj do grupy*** i wpisujemy w oknie nazwę grupy np: *klasa1.*

Testujemy możliwość logowania nowego użytkownika do komputera przyłączonego do domeny. W oknie maszyny z Windows 10: przełączamy użytkownika (wylogować użytkownika root) i logujemy się na nowego utworzonego w domenie !!). Wszystko działa, posiadamy domenę, komputery do niej podpięte i użytkowników, nad którymi poprzez Serwer mamy pełną kontrolę.

W kolejnym kroku można edytować zasady (co można a co nie) dla grup, użytkowników. Zasady grupy, użytkowników dokonujemy na maszynie z Windows Serwer. W ***Serwer Manager w Narzędziach wybieramy zarządzanie zasadami grupy (Group Policy Managment).***

Modelowanie zasad grupy: w domenie mamy dostęp do jednostek organizacyjnych utworzonych wcześniej (uczniowie, nauczyciele i administracja), grup lub użytkowników. Możemy tutaj dodawać, edytować i usuwać zasady dla każdego elementu.

Każda zmiana zasad wymaga wymuszenie poprawności na każdym komputerze podpiętym do domeny, aby ten skutek uzyskać należy zresetować wszystkie komputery w domenie, lub ręcznie na każdym wymusić: (w konsoli cmd wpisujemy) ***gpupdate /force***

h. Zasady grup i użytkowników:
    - Na Windows Serwer uruchamiamy ***Menadżer Serwera*** (***Serwer Manager),*** ***wybieramy narzędzia -> zarządzanie zasadami grupy, wybieramy domenę: SZKOLA.LOCAL,***
    - W lewym oknie klikamy 2x szybko nazwie domeny np.: ***Las:nazwa_domeny***
    - Z rozwiniętej listy wybieramy Domeny, klikamy 2x szybko na ***nazwa_domeny*** (rozwijamy nowe pozycje), nowe pozycje to np.: ***Default Domain Policy*** – klikamy PPM i edytuj, pojawi się nowe okno, w którym z lewej strony pojawią się 2 główne pozycje ***User i Computer Configuration***, wybieramy ***User Configuration*** i pozycję ***Zasady (Policies)***
    - ***User Configuration***, możemy dalej rozwijać poszczególne elementy aż do włączenia/wyłączenia zasady, poniżej przykłady zasad i schemat rozwijania poszczególnej zasady ..-> .. -> .. -> …etc

Poniżej znajdziecie **kilkanaście przykładowych ustawień**, które ograniczają użytkownikom dostęp do poszczególnych elementów systemu operacyjnego oraz zmieniają konkretne ustawienia (opis tylko w języku angielskim):

1. Blokada całego Panelu Sterowania:

User Configuration -> Administrative Templates -> Control Panel -> Prohibit access to Control Panel and PC settings -> ENABLED

2. Ukrycie poszczególnych elementów w Panelu Sterowania:

User Configuration -> Administrative Templates -> Control Panel -> Hide specified Control Panel items -> ENABLED *(po włączeniu opcji wprowadzamy nazwy elementów, które chcemy zablokować)*

3. Blokada ustawień ekranu:

User Configuration -> Administrative Templates -> Control Panel -> Display -> Disable the Display Control Panel -> ENABLED

4. Blokada zmiany tapety:

User Configuration -> Administrative Templates -> Control Panel -> Personalization -> Prohibit changing desktop background -> ENABLED

5. Blokada usuwania drukarek:

User Configuration -> Administrative Templates -> Control Panel -> Printers -> Prevent deletion of printers -> ENABLED

6. Wyłączenie ikon Komputer, Sieć, Kosz z pulpitu:

User Configuration -> Administrative Templates -> Desktop-> Hide and disable all items on the desktop -> ENABLED

7. Ustawienie konkretnej tapety pulpitu:

User Configuration -> Administrative Templates -> Desktop-> Desktop -> Desktop Wallpaper -> ENABLED *(po włączeniu tej opcji podajemy ścieżkę do konkretnej tapety)*

8. Usunięcie elementu *Uruchom* z Menu Start:

User Configuration -> Administrative Templates -> Start Menu and Taskbar -> Remove Run menu form Start Menu -> ENABLED

9. Usunięcie elementu *Zablokuj komputer* po wciśnięciu CTRL + ALT + DEL:

User Configuration -> Administrative Templates -> System -> Ctrl+Alt+Del Options -> Remove Lock Computer -> ENABLED

10. Usunięcie elementu *Wyloguj* po wciśnięciu CTRL + ALT + DEL:

User Configuration -> Administrative Templates -> System -> Ctrl+Alt+Del Options -> Remove Logoff -> ENABLED

11. Blokada odczytu danych z dysków zewnętrznych:

User Configuration -> Administrative Templates -> System -> Removable Storage Access -> Removable Disks: Deny read access -> ENABLED

12. Limit wielkości profilu użytkownika:

User Configuration -> Administrative Templates -> System -> User Profiles -> Limit profile size -> ENABLED *(po włączeniu tej opcji określamy wielkość maksymalną profilu)*

13. Blokada dostępu do edycji rejestru:

User Configuration -> Administrative Templates -> System -> Prevent access to registry edition tools -> ENABLED

14. Blokada dostępu do wiersza poleceń:

User Configuration -> Administrative Templates -> System -> Prevent access to command prompt -> ENABLED

15. Uruchamianie tylko wybranych aplikacji:

User Configuration -> Administrative Templates -> System -> Run only specified Windows applications -> ENABLED *(po włączeniu tej opcji podajemy nazwy plików uruchomieniowych aplikacji)*

16. Blokada wyświetlania wybranych partycji w Eksploratorze Windows:

User Configuration -> Administrative Templates -> Windows Components -> File Explorer -> Hide these specified drivers in My Computer *(po włączeniu tej opcji wybieramy właściwe ustawienia)*

To oczywiście niewielki wycinek wielkich możliwości konfiguracyjnych jakie dają **Zasady Grupy**. Ustawień w samych **Szablonach Administracyjnych** (ang. **Administrative Templates**) jest ponad **150**0. Do tego dochodzą jeszcze **Preferencje Zasad** (ang. **Preferences**), **Ustawienia Oprogramowania** (ang. **Software Settings**) oraz **Ustawienia Windows** (ang. **Windows Settings**). Za ich pomocą można, np. **zdalnie instalować oprogramowanie**, **mapować drukarki** i **foldery**, czy **automatycznie kopiować na serwer zawartość katalogów z profili użytkowników**. Zachęcam do samodzielnej „zabawy" z Zasadami Grupy i testowanie poszczególnych ustawień.

Zadanie do samodzielnego wykonania:

A1. Utwórz nowy **las** oraz **domenę** o nazwie ***firma.com***

2. Ustaw długość haseł dla użytkowników w domenie na min. **4 znaki** oraz **wyłącz złożoność** tych haseł.

3. Podłącz do domeny 1 **komputer kliencki** i nadaj mu nazwę: **STACJANR1**.

4. Utwórz i skonfiguruj konta użytkowników pracujących w domenie wg podanych założeń:

4.1. Utwórz **jednostkę organizacyjną** o nazwie ***workers***, a w niej:

4.1.1. Utwórz konto ***Maria Skłodowska*** z loginem ***ksiegowy*** oraz hasłem ***B456***

4.1.2. Utwórz konto ***Zofia Antonina*** z loginem ***kadrowy*** oraz hasłem ***C789***

4.2. Konta ***księgowy*** oraz ***kadrowy*** skonfiguruj tak, aby możliwe było logowanie **od poniedziałku do piątku** w godzinach **od 8:00 do 16:00**, tylko na komputerze **STACJA1.**

4.3. Utwórz **jednostkę organizacyjną** o nazwie ***owners***, a w niej: 4.3.1. Utwórz konto ***Adam Słodowy*** z loginem ***wlasciciel*** oraz hasłem ***A123***

A2. Dla utworzonych użytkowników zaprezentuj sposób działania zasad w formie zrzutów ekranu dla **…4…** wybranych/dowolnych zasad.

4. Sposób weryfikacji realizacji laboratorium przez prowadzącego :

Aby przyznać punkty i zaliczyć laboratorium studentowi, musi on zrealizować krok po kroku punkt 3 laboratorium, każdy etap w sprawozdaniu musi być opatrzony zrzutem ekranu wraz z opisem realizacji i efektu działania. Na koniec musi wykonać i poprzez zrzuty ekranu udokumentować poprawną realizację zadania do samodzielnego wykonania.

5. Zabezpieczenie przed kopiowaniem sprawozdań

Każdy student będzie pracował na swoim obrazie zarówno Windows Serwer jak i Windows 7/10, utworzone tam konta będą jego własnością dlatego w łatwy sposób można zweryfikować czy zrzuty ekranu i wyniki prac wynikają z samodzielności czy też nie.

6. Wymagania odnośnie infrastruktury sprzętowej i programowej w laboratorium

Wymagany jest VirtualBox, obraz Windows Server 2012 R2, obraz Windows 10 min. Wersja PRO – każdy student musi posiadać swoje obrazy !! nie może być jak teraz że jest jeden na komputerze i każdy ma do niego dostęp !!Każdy pracuje na swoich obrazach, aby uniknąć sytuacji że jedna grupa zrobi i późniejsze mają gotowe i spreparowane obrazy.