Lekcja: Zarządzanie zasadami grup. Polityka haseł.

Cel Ogólny lekcji: Zapoznanie uczestników z zarządzaniem zasadami grup oraz polityką haseł w serwerach Windows, skupiając się na bezpieczeństwie i efektywności w środowisku serwerowym.

Cele szczegółowe:

1. **Zarządzanie zasadami grup:**

- Wyjaśnienie, czym są zasady grup i jak wpływają na proces administracyjny.

2. **Zalety centralizacji zarządzania:**

- Przedstawienie korzyści z centralizacji zarządzania za pomocą zasad grup w serwerach Windows.

3. **Kontrola dostępu:**

- Omówienie sposobów kontrolowania dostępu przy użyciu zasad grup.

4. **Automatyzacja procesów:**

- Wyjaśnienie roli automatyzacji procesów za pomocą zasad grup.

5. **Wspieranie zgodności:**

- Przedstawienie, w jaki sposób zasady grup wspierają zgodność ze standardami bezpieczeństwa.

6. **Elementy zarządzania zasadami grup:**

- Wyjaśnienie roli elementów, takich jak grupy i zasady grupy.

7. **Pierwotność i dziedziczenie:**

- Omówienie, jak działa hierarchia zasad grup i dziedziczenie ustawień.

8. **Dostęp i edycja:**

- Wskazanie, jak uzyskać dostęp do edycji zasad grupy.

W wyniku lekcji uczestnicy powinni zrozumieć kluczowe koncepcje związane z zarządzaniem zasadami grup i polityką haseł w środowisku serwerowym opartym na Windows.

Wprowadzenie: W dzisiejszej lekcji zajmiemy się teoretycznymi aspektami zarządzania zasadami grup oraz polityką haseł w serwerach opartych na systemach Windows 2016, 2019 i 2022. Dowiemy się, jak te koncepcje wpływają na organizację, bezpieczeństwo i efektywność w kontekście środowiska serwerowego.

Część 1: Zarządzanie zasadami grup w serwerach Windows

A. Definicja:

Zarządzanie zasadami grup w serwerach Windows to proces, w ramach którego administratorzy definiują i kontrolują ustawienia dla użytkowników oraz komputerów w domenie lub sieci.
Pozwala to na centralne zarządzanie dostępem, uprawnieniami i konfiguracją. Zasady grup to narzędzie administracyjne, które pozwala na centralne zarządzanie ustawieniami systemu i użytkowników w sieci.

B. Zalety:

a) Centralizacja zarządzania w kontekście zasad grup w serwerach Windows:

Zasady grupy to sposób na ustawianie reguł i ograniczeń dla komputerów i użytkowników w domenie. Możesz zmieniać zasady grupy za pomocą Edytora obiektów zasad grupy.

Centralizacja zarządzania to zaleta zasad grupy, ponieważ możesz kontrolować wszystko z jednego miejsca. Nie musisz zmieniać ustawień na każdym komputerze osobno. Centralizacja zarządzania pomaga też w rozwiązywaniu problemów z zasadami grupy. W przypadku zasad grup w serwerach Windows 2016, 2019 i 2022, centralizacja ma wiele korzyści:

1. **Jednolite podejście**: to zaleta zasad grupy, ponieważ możesz ustawić takie same zasady i ustawienia dla wielu użytkowników lub komputerów w domenie. Nie musisz zmieniać każdego ustawienia osobno. Możesz stworzyć obiekt zasad grupy i przypisać go do jednostki organizacyjnej lub grupy. Wtedy wszystkie obiekty w tej jednostce lub grupie będą miały taką samą konfigurację.

2. **Skuteczne zarządzanie uprawnieniami**: Zasady grupy to sposób na określanie, kto i jak może korzystać z zasobów, takich jak pliki, foldery, drukarki czy aplikacje. Możesz używać jednostek organizacyjnych lub grup, żeby podzielić obiekty w domenie na kategorie. Jednostki organizacyjne tworzą drzewo obiektów i pozwalają na dawanie uprawnień innym administratorom. Grupy łączą obiekty, które mają podobne potrzeby dostępu do zasobów.
Możesz przypisać obiekt zasad grupy do jednostki organizacyjnej lub grupy, żeby ustawić zasady konfiguracji i bezpieczeństwa dla obiektów w nich. Centralizacja zarządzania to zaleta zasad grupy, ponieważ możesz kontrolować dostęp do zasobów z jednego miejsca.

Nie musisz sprawdzać każdego obiektu osobno. Centralizacja zarządzania ułatwia też naprawianie błędów i zapobieganie nadużyciom.

3. **Ułatwiona aktualizacja i zmiany**: Zasady grupy pozwalają na łatwe zmiany w ustawieniach dla jednostek organizacyjnych lub grup. Możesz edytować obiekt zasad grupy, żeby zmienić dostęp do zasobów lub politykę bezpieczeństwa dla obiektów w jednostce organizacyjnej lub grupie. Zmiany będą automatycznie zastosowane do wszystkich użytkowników lub komputerów w nich. Nie musisz zmieniać ustawień na każdym urządzeniu osobno.

4. **Minimalizacja ryzyka błędów**: Dostęp warunkowy pozwala na ograniczenie dostępu do zasobów w zależności od różnych sygnałów, np. lokalizacji, aplikacji czy tożsamości. Możesz użyć grup zabezpieczeń Azure AD lub grup Microsoft 365, żeby wybrać, kto ma być objęty lub wyłączony z zasad dostępu warunkowego. Dzięki temu możesz lepiej chronić swoje dane i zasoby przed nieautoryzowanym dostępem. Nie musisz ustawiać zasad dla każdego użytkownika osobno.

5. **Efektywność czasowa**: Zarządzanie zasadami grupy pozwala na zmianę ustawień dla wielu użytkowników i komputerów naraz. Możesz tworzyć niestandardowe jednostki organizacyjne w domenie, żeby lepiej podzielić i zarządzać użytkownikami. Możesz też zmieniać zasady dotyczące np. haseł, blokady konta czy panelu sterowania. Windows Server 2016 ma też ulepszone algorytmy synchronizacji czasu, które zapewniają dokładność i spójność czasu na wszystkich maszynach wirtualnych.

6. **Ułatwienie audytu i raportowania**: Centralizacja ułatwia sprawdzanie i kontrolowanie zasad i dostępów. Możesz szybko dowiedzieć się, kto ma dostęp do czego i co się zmieniło. Możesz też użyć programu ADAudit Plus, żeby śledzić i raportować różne aktywności na serwerach Windows, np. logowanie i wylogowanie użytkowników, usługi terminalowe, procesy, zadania, drukarki czy urządzenia USB.

Podsumowując, centralizacja zarządzania za pomocą zasad grup w serwerach Windows 2016, 2019 i 2022 przyczynia się do spójności, bezpieczeństwa i efektywności w zarządzaniu środowiskiem serwerowym. Dzięki niej administratorzy mogą skutecznie wprowadzać zmiany, kontrolować dostępy i minimalizować ryzyko błędów przy jednoczesnym oszczędzaniu czasu i wysiłku.

b) Kontrola dostępu w kontekście zasad grup w serwerach Windows:

Kontrola dostępu to sposób na określenie, kto może korzystać z czego. Możesz używać grup do zarządzania zasobami, np. plikami, folderami, drukarkami czy aplikacjami. Możesz też używać zasad grupy do zmiany ustawień dla użytkowników, np. haseł, blokady konta czy panelu sterowania.

Możesz tworzyć jednostki organizacyjne w domenie, żeby lepiej podzielić i zarządzać grupami i zasadami. Możesz też używać grup z Azure Active Directory i Microsoft 365, żeby zabezpieczać dostęp do zasobów w chmurze.

1. **Zastosowanie grup zabezpieczeń usługi Azure Active Directory (Azure AD) i Grupy Microsoft 365:** Zasady grupy mogą współpracować z grupami w chmurze. To pomaga zabezpieczać dostęp do zasobów w Azure i Microsoft 365, np. pliki w OneDrive czy SharePoint. To ułatwia zarządzanie dostępem w środowiskach hybrydowych.

2. **Obiekty zasad grupy w jednostkach organizacyjnych:** Administratorzy mogą zmieniać zasady grupy dla różnych jednostek organizacyjnych. To pozwala dostosować ustawienia dla różnych użytkowników. Na przykład, można zmieniać zasady dotyczące haseł, dostępu czy blokady konta.

3. **Kontrola dostępu do zasobów:** Zasady grupy pozwalają ustawić, kto ma dostęp do czego Administratorzy mogą tworzyć grupy według ról lub funkcji. Potem mogą im dać odpowiednie uprawnienia.

4. **Blokada panelu sterowania, zasady haseł i zasady blokady konta:** Zasady grupy pozwalają ustawić reguły dla różnych rzeczy. Na przykład, można zablokować Panel sterowania, wymagać hasła lub reagować na błędne logowania. To pomaga skonfigurować system bezpiecznie i dostępnie.

Podsumowując, kontrola dostępu w kontekście zasad grup w serwerach Windows 2016, 2019 i 2022 pozwala administratorom precyzyjnie zarządzać, kto ma dostęp do zasobów oraz jakie uprawnienia są nadawane. Integracja z chmurą za pomocą grup zabezpieczeń Azure AD i Grup Microsoft 365 oraz możliwość definiowania specyficznych zasad dla jednostek organizacyjnych dodatkowo wzbogacają możliwości kontroli dostępu w dynamicznych środowiskach.

c) **Automatyzacja procesów administracyjnych za pomocą zasad grup w serwerach Windows**:
Zasady grupy to funkcja Windows do automatycznego zarządzania ustawieniami i zasadami dla urządzeń i użytkowników w Active Directory. Można tworzyć i zmieniać obiekty zasad grupy (GPO) w jednostkach organizacyjnych (OU) i przypisywać je do grup. Configuration Manager i Desktop Analytics używają zasad grupy do ustawiania zasad Windows w rejestrze.
Zasady grupy pomagają w rozwiązywaniu problemów i bezpieczeństwie danych.

1. **Automatyczne przypisywanie zasad do urządzeń i użytkowników:** Zasady grupy to sposób na automatyczne ustawianie zasad dla grup urządzeń lub użytkowników.
Na przykład, możemy ustawić zasady bezpieczeństwa dla wszystkich komputerów w jednej jednostce organizacyjnej. To zaaplikuje zasady do każdego urządzenia w tej grupie.

2. **Tworzenie i edycja obiektów zasad grupy w jednostkach organizacyjnych:**
Zasady grupy to sposób na automatyczne ustawianie zasad dla nowych urządzeń lub użytkowników. Administratorzy mogą ustawić zasady w jednostkach organizacyjnych i przypisać je do grup. To pozwala na uniknięcie ręcznego zmieniania ustawień dla każdego urządzenia czy użytkownika.

3. **Skalowalność i spójność:** Zasady grupy to sposób na łatwe i spójne zarządzanie. Nie ważne, ile jest urządzeń czy użytkowników, zasady grup pozwala zastosować te same zasady i ustawienia, co zmniejsza ryzyko błędów i różnych konfiguracji.

4. **Usprawnienie procesów:** Zasady grupy to sposób na szybkie i łatwe zarządzanie.
Zamiast ręcznie zmieniać ustawienia na każdym urządzeniu lub dla każdego użytkownika, administratorzy mogą ustawić jedną zasadę grupy, która zostanie automatycznie zastosowana do odpowiednich grup.

5. **Kontrola i audyt:** Zasady grupy to sposób na lepszą kontrolę i audyt zarządzania.
Zmiany w zasadach grup są rejestrowane, co ułatwia sprawdzanie i audyt zmian.

Podsumowując, automatyzacja procesów administracyjnych poprzez zasady grup w serwerach Windows 2016, 2019 i 2022 pozwala na spójność, skalowalność i usprawnienie zarządzania.
To narzędzie umożliwia administratorom efektywne wprowadzanie zmian, przypisywanie ustawień i zasad oraz minimalizowanie ryzyka ludzkich błędów.

d) **Zachowanie zgodności ze standardami bezpieczeństwa za pomocą zasad grup w serwerach Windows**:

Zasady grup w serwerach Windows 2016, 2019 i 2022 zapewniają spójne i konsekwentne stosowanie zasad, co jest niezwykle istotne dla zachowania odpowiedniego poziomu bezpieczeństwa.

1. **Spójność i konsekwencja:** Zasady grupy to sposób na ustawianie zasad dla grup użytkowników lub komputerów. To oznacza, że wszyscy użytkownicy czy urządzenia w danej grupie będą mieć te same zasady i zabezpieczenia. Zasady grup wykorzystują system zarządzania na serwerze, który rozsyła zasady na komputery klienckie. Zasady grup przechowywane są w obiektach zasad grupy (GPO), które są powiązane z obiektami w Active Directory (AD), takimi

jak jednostki organizacyjne (OU), domeny lub lokalizacje. Dzięki temu możemy łatwo zarządzać systemem, bezpieczeństwem, oprogramowaniem czy skryptami dla różnych grup użytkowników lub komputerów w naszej sieci.

2. **Wspieranie zgodności regulacji:** Zasady grup pomagają w zabezpieczaniu i zarządzaniu danymi zgodnie z regulacjami, takimi jak GDPR. Za pomocą zasad grup można ustawić zasady, które ograniczają dostęp do danych, szyfrują dane i pokazują, że podmioty przestrzegają regulacji i chronią dane.

GDPR to Rozporządzenie Ogólne o Ochronie Danych (ang. General Data Protection Regulation), które obowiązuje w Unii Europejskiej i dotyczy wszystkich danych osobowych osób, które podlegają jego zasięgowi. Regulacja wymaga od podmiotów odpowiedzialnych za przetwarzanie danych osobowych zapewnienia ich bezpieczeństwa, poufności i integralności, ale ma też różne zakresy zastosowania, zgody, praw osób, których dane dotyczą i sankcji.

3. **Silne hasła i polityka haseł:** Zasady grup pomagają w zabezpieczaniu kont użytkowników zgodnie z standardami bezpieczeństwa. Za pomocą zasad grup można ustawić wymagania dotyczące haseł, takie jak długość, znaki i zmiana haseł. Silne hasła to takie, które są trudne do odgadnięcia lub odzyskania. Silne hasła powinny być unikalne, niepowiązane z danymi osobowymi, długie (12 znaków lub więcej) i zróżnicowane (małe i duże litery, cyfry i znaki specjalne). Polityka haseł to zbiór zasad i procedur, które mówią, jak tworzyć, przechowywać i używać haseł w organizacji. Polityka haseł powinna być jasna, aktualna i egzekwowana.

4. **Ochrona zasobów:** Zasady grup pomagają w kontrolowaniu dostępu do zasobów, takich jak foldery, pliki czy drukarki, co chroni dane i informacje. Zasady grup można użyć do zwiększenia bezpieczeństwa, na przykład do wyłączenia starych protokołów, zablokowania pewnych zmian i wymuszenia silnych haseł. Kontrola dostępu to proces, który sprawdza, czy użytkownik zasobów jest tym, kim być powinien, i czy ma prawa dostępu do danych na podstawie zasad. Kontrola dostępu zapobiega nieautoryzowanemu użyciu danych przez osoby nieuprawnione.

5. **Blokady po nieudanych próbach logowania:** Zasady grup pomagają w ustawieniu polityki blokady konta po wielu błędnych logowaniach. To zabezpieczenie pomaga w zapobieganiu atakom typu “brute force”. Blokada konta polega na tymczasowym zablokowaniu logowania dla użytkownika, jeśli wpisał on złe dane zbyt wiele razy. Blokadę konta można ustawić za pomocą narzędzi w panelu sterowania lub wiersza polecenia. Blokada konta może być synchronizowana między centrach danych Azure AD, aby zapewnić spójną ochronę. Blokada konta może być też ustawiona pod względem czasu, częstotliwości i informowania użytkownika.

6. **Automatyzacja reakcji na naruszenia:** Zasady grup pomagają w automatycznym reagowaniu na naruszenia bezpieczeństwa, takie jak zablokowanie konta użytkownika lub zmiana haseł. To zapewnia szybką i skuteczną reakcję na zagrożenia. Automatyzację reakcji na naruszenia można ustawić za pomocą usługi zasady grupy (GPSvc), która wykonuje obiekty zasad grupy na komputerach klienckich. Automatyzacja reakcji na naruszenia może też pomóc w zgłaszaniu naruszeń organom i osobom, których dotyczy, zgodnie z prawem. Automatyzacja reakcji na naruszenia może także współpracować z systemami zarządzania tożsamością i dostępem (IAM), które nadają użytkownikom tylko potrzebne uprawnienia i monitorują ich aktywność.

Podsumowując, zasady grup w serwerach Windows umożliwiają organizacjom skuteczne zachowanie zgodności ze standardami bezpieczeństwa. Poprzez stosowanie spójnych zasad, silnych haseł i kontrolowanego dostępu do zasobów, organizacje mogą utrzymywać wysoki poziom bezpieczeństwa i zabezpieczenia danych, jednocześnie spełniając wymogi regulacji.

C. **Elementy:**

a) **Grupy**: Za pomocą usługi Active Directory (AD) można tworzyć grupy na podstawie ról lub struktury organizacyjnej w serwerach Windows. AD to system zarządzania tożsamością i dostępem w sieciach Windows. AD pozwala na tworzenie jednostek organizacyjnych (OU), które są kontenerami dla obiektów takich jak użytkownicy, komputery, grupy i inne.
Za pomocą zasad grupy (GPO) można określać ustawienia konfiguracyjne dla obiektów AD. GPO mogą dotyczyć zasad bezpieczeństwa, preferencji użytkowników i innych aspektów systemu.
Tworzenie grup na podstawie ról lub struktury organizacyjnej w serwerach Windows może być łatwiejsze przez użycie narzędzi administracji zdalnej serwera (RSAT), które pozwalają na zdalne zarządzanie serwerem z komputera klienckiego.

b) **Zasady grup**: Za pomocą zasady grupy (GPO) można ustawiać zabezpieczenia i dostosowywać środowisko użytkowników w określonych grupach w serwerach Windows. GPO to zestaw ustawień konfiguracyjnych dla obiektów usługi Active Directory. GPO można tworzyć i edytować za pomocą narzędzia Zarządzanie zasadami grupy (GPMC), które pozwala też przypisywać GPO do jednostek organizacyjnych (OU) i sprawdzać wynikowe zasady dla obiektów AD. GPO mogą dotyczyć różnych aspektów systemu, takich jak zabezpieczenia usług, dane diagnostyczne, zasady haseł i blokady konta i wiele innych.

Zasady grupy to narzędzie do zarządzania ustawieniami komputerów i użytkowników w sieci Windows. Zasady grupy są zapisane w obiektach zasad grupy (GPO), które są powiązane z jednostkami organizacyjnymi (OU) w usłudze Active Directory (AD). Aby zarządzać zasadami grupy, używamy

konsoli zarządzania zasadami grupy (GPMC). Zasady grupy dla Windows Server 2016, 2019 i 2022 mogą się nieco różnić, dlatego należy sprawdzać dokumentację dla każdej wersji systemu.

Zasady grupy mają dwa rodzaje ustawień:

- ustawienia komputera - dotyczą całego komputera i są stosowane przy uruchomieniu systemu
- ustawienia użytkownika - dotyczą tylko zalogowanego użytkownika i są stosowane przy logowaniu

W zasadach grupy możesz wybrać różne ustawienia dla komputerów i użytkowników (np. zablokować dostęp do rejestru, ograniczyć uruchamianie aplikacji itp.). Niektóre ustawienia są dostępne dla obu rodzajów, a niektóre tylko dla jednego (np. przekierowanie folderu tylko dla użytkownika, a instalacja oprogramowania tylko dla komputera).

Omówienie konsoli zarządzania zasadami grupy.

Konsola zarządzania zasadami grupy to narzędzie, które pozwala tworzyć, edytować i zarządzać obiektami zasad grupy (GPO) dla domeny i jednostek organizacyjnych (OU). Możesz uruchomić konsolę GPO wpisując gpmc.msc w oknie dialogowym Uruchom… lub wybierając Zarządzanie zasadami grupy z menu Narzędzia administracyjne.

W konsoli GPO możesz znaleźć różne elementy, np.:

- Default Domain Policy - to domyślne zasady dla całej domeny.
- Domain Controllers - to jednostka organizacyjna dla kontrolerów domeny (naszych serwerów).
- Group Policy Objects - to folder z wszystkimi zasadami, które tworzymy i stosujemy.
- WMI Filters - to folder z filtrami WMI, które pozwalają na stosowanie zasad w zależności od właściwości komputera.
- Starter GPOs - to folder z zasadami dla komputerów z systemami Windows (trzeba je włączyć klikając w Create starter GPOs).
- Site - to element z zasadami dla różnych lokalizacji w domenie.
- Group Policy Modeling - to narzędzie do projektowania zasad.
- Group Policy Result - to narzędzie do sprawdzania wyników działania zasad.

Zasady grupy mogą nie działać od razu, jeśli użytkownik jest już zalogowany. Aby zasady działały od razu, możesz użyć polecenia gpupdate /force na stacji roboczej. Albo poczekać na automatyczne odświeżenie zasad lub wylogować i zalogować się ponownie.

Domyślnie zasady grupy są odświeżane w tle co 90 minut z losowym przesunięciem od 0 do 30 minut. Możesz jednak zmienić interwał odświeżania zgodnie z wymaganiami. Aby to zrobić, możesz użyć

Edytora zasad grupy lub Edytora rejestru. W Edytorze zasad grupy musisz przejść do opcji Konfiguracja komputera > Szablony administracyjne > Zasady grupy i kliknąć dwukrotnie zasadę **Ustaw interwał odświeżania zasad grupy dla komputerów**.

Omówienia elementów konsoli służących do zarządzania pojedynczym obiektem.

Obiekt zasad grupy (GPO) to zbiór ustawień, które możesz zastosować do użytkowników i komputerów w domenie. Możesz zarządzać GPO za pomocą konsoli MMC lub polecenia gpupdate. Możesz też kopiować, tworzyć kopie zapasowe, przywracać, importować, zapisywać raporty, usuwać i zmieniać nazwy GPO. Ważne jest, aby znać pierwszeństwo i dziedziczenie zasad grupy, aby wiedzieć, które ustawienia będą obowiązywać.

Obiekt to zbiór zasad przez nas zdefiniowanych, zapisanych w folderze Group Polisy Object.
Aby dostać się do elementów zarządzania obiektem, klikamy prawym przyciskiem myszy na jego nazwę, znajdziemy tam m.in.:

- Copy (kopiuj) - polecenie służące do kopiowania obiektu, przydatne wówczas, kiedy chcemy stworzyć obiekt, którego ustawienia mają bazować na ustawieniach innych obiektów
- Back up (kopia zapasowa) - polecenie służące do tworzenia kopii zapasowej obiektu, kopiujące nie tylko sam obiekt, ale również łącza do niego, uprawnienia oraz dodatkowe pliki
- Restore From Backup (przywróć z kopii zapasowej) - polecenie służące do przywracania obiektu z stworzonej uprzednio kopii zapasowej
- Import Settings (importuj ustawienia) - polecenie służące do kopiowania samych ustawień zapisanych w obiekcie, bez łącz i uprawnień
- Save Report (zapisz raport) - polecenie służące do zapisywania raportu do pliku HTML
- Delete (usuń) - polecenie służące do usunięcia obiektu wraz z łączami i uprawnieniami
- Rename (zmień nazwę) - polecenie służące do zmiany nazwy obiektu

Pierwszeństwo przetwarzania zasad

Kolejność przetwarzania zasad grupy (GPO) określa, które ustawienia będą obowiązywać, gdy występują konflikty między różnymi GPO. Domyślnie GPO przetwarzane są w następującej kolejności:

1. Lokalne GPO na komputerze

2. GPO na poziomie lokacji
3. GPO na poziomie domeny
4. GPO na poziomie jednostki organizacyjnej

Możesz zmienić kolejność przetwarzania GPO w konsoli Zarządzanie zasadami grupy lub za pomocą polecenia gpupdate

Dziedziczenie

Zasady grupy (GPO) są dziedziczone przez jednostki organizacyjne (OU) od domeny i lokacji.

To znaczy, że ustawienia zastosowane na wyższym poziomie będą obowiązywać na niższym poziomie, chyba że zostaną nadpisane lub zablokowane. Na przykład, jeśli ustawisz blokadę ekranu po 60 sekundach dla domeny, to będzie ona dotyczyć wszystkich komputerów i użytkowników w tej domenie.

Możesz wyłączyć dziedziczenie GPO dla danej domeny lub OU w konsoli Zarządzanie zasadami grupy. Wtedy ustawienia z wyższego poziomu nie będą wpływać na niższy poziom. Aby to zrobić, kliknij prawym przyciskiem myszy na domenę lub OU, wybierz Właściwości, a następnie przejdź do zakładki Zasady grupy. Tam możesz zaznaczyć opcję Blokuj dziedziczenie.

Wyłączymy dziedziczenie

Możesz zablokować dziedziczenie zasad grupy (GPO) dla kontenera (OU), klikając na niego prawym przyciskiem myszy i wybierając opcję Blokuj dziedziczenie. Wtedy GPO z wyższego poziomu nie będą wpływać na ten kontener. Obiekt Domyślna zasada domeny nie będzie widoczny dla tego kontenera.

Blokowanie dziedziczenia jest opcją, której należy używać ostrożnie lub wcale. Może ona zmienić kolejność przetwarzania GPO i spowodować niechciane efekty. Lepiej jest mieć dobrze zaprojektowaną strukturę OU i stosować GPO na odpowiednim poziomie.

Kontenery (OU) służą do organizowania użytkowników i komputerów w domenie i stosowania GPO na nich. Grupy użytkowników służą do nadawania uprawnień i dostępu do zasobów dla wielu użytkowników naraz. To są dwa różne obiekty w Active Directory.

Przekierowanie folderu

Jeśli chcesz, aby użytkownicy domeny mieli swoje pliki i dokumenty zawsze dostępne w sieci, możesz użyć dwóch funkcji: przekierowania folderu lub profilu mobilnego.

Przekierowanie folderu pozwala na wybór, które foldery z profilu użytkownika będą zapisywane na serwerze. Na przykład, możesz przekierować folder Moje dokumenty do udostępnionego folderu w sieci. Wtedy użytkownik będzie miał dostęp do swoich dokumentów z każdego komputera w domenie.

Profil mobilny to kopia całego profilu użytkownika, która jest zapisywana na serwerze. Każdy plik i ustawienie z profilu jest synchronizowany z serwerem przy logowaniu i wylogowaniu się użytkownika. Wtedy użytkownik będzie miał taki sam pulpit i ustawienia na każdym komputerze w domenie.

W konsoli GPO możesz zmieniać różne ustawienia zasad grupy dla komputerów i użytkowników, np. blokować panel sterowania, zmieniać zasady haseł lub blokady konta itp1. Aby sprawdzić, jakie ustawienia są aktywne dla danego komputera lub użytkownika, możesz użyć narzędzia Wynikowy zestaw zasad.

Zasady grupy dla Windows Server 2016, 2019 i 2022 są podobne, ale nie identyczne. Niektóre ustawienia zasad grupy mogą być dostępne tylko dla określonej wersji systemu Windows lub mogą mieć różne nazwy lub wartości. Dlatego zaleca się, aby sprawdzać dokumentację dla każdej wersji systemu Windows przed wprowadzaniem zmian w zasadach grupy.

c) **Uprawnienia**: Określanie, jakie czynności i zasoby są dostępne dla danej grupy w serwerach Windows jest procesem, który pozwala na nadawanie uprawnień i kontrolowanie dostępu do obiektów systemowych i sieciowych. Może być realizowane na dwa sposoby: za pomocą użytkowników i grup lokalnych lub za pomocą użytkowników i grup Active Directory. Użytkownicy i grupy lokalne są tworzone i zarządzane na poziomie pojedynczego serwera bez domeny i mają uprawnienia tylko do tego serwera. Użytkownicy i grupy Active Directory są tworzone i zarządzane na poziomie kontrolera domeny i mają uprawnienia do wszystkich obiektów w domenie. Określanie, jakie czynności i zasoby są dostępne dla danej grupy w serwerach Windows może być również ułatwione przez użycie zasady grupy aplikacji Ustawienia, która pozwala na pokazywanie lub ukrywanie określonych stron aplikacji i ustawień dla użytkowników.

Część 2: Polityka haseł w serwerach Windows

A. Definicja:

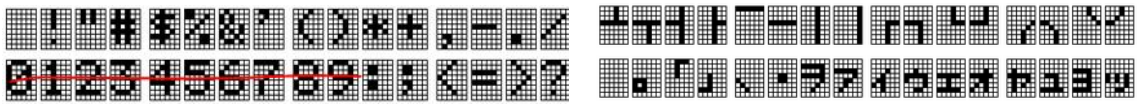
Polityka haseł w serwerach Windows to zestaw reguł określających wymagania dotyczące tworzenia, przechowywania i używania haseł przez użytkowników.

Polityka haseł w serwerach Windows ma na celu zwiększenie bezpieczeństwa i zapobieganie atakom na konta użytkowników.

Polityka haseł w serwerach Windows może obejmować takie elementy jak:

- minimalna długość hasła oznacza, że system wymaga, aby hasło użytkownika miało co najmniej określoną liczbę znaków. Minimalna długość hasła jest jednym z ustawień zasad haseł, które można skonfigurować dla domyślnej zasady hasła domeny lub dla precyzyjnych zasad haseł (FGPP) za pomocą obiektów polityki haseł (PSO). Minimalna długość hasła ma na celu zapobieganie użyciu zbyt prostych lub łatwych do odgadnięcia haseł, które mogą być narażone na ataki siłowe lub słownikowe. Domyślnie system Windows ustawia minimalną długość hasła na 7 znaków, ale można zmienić tę wartość w ustawieniu zasady Minimum password length (Minimalna długość hasła). W niektórych nowszych wersjach systemu Windows możliwe jest również wymuszenie minimalnej długości hasła co najmniej 15 znaków.
- maksymalny wiek hasła oznacza, że system wymusza regularną zmianę hasła przez użytkownika po upływie określonego czasu. Maksymalny wiek hasła jest jednym z ustawień zasad haseł, które można skonfigurować dla domyślnej zasady hasła domeny lub dla precyzyjnych zasad haseł (FGPP) za pomocą obiektów polityki haseł (PSO). Maksymalny wiek hasła ma na celu zapobieganie użyciu przestarzałych lub skompromitowanych haseł, które mogą być narażone na ataki. Domyślnie system Windows ustawia maksymalny wiek hasła na 42 dni, ale można zmienić tę wartość w ustawieniu zasady Maximum password age (Maksymalny wiek hasła).
- historia hasła oznacza, że system zapamiętuje określoną liczbę ostatnio używanych haseł przez użytkownika i nie pozwala na ich ponowne użycie przy zmianie hasła1. Historia hasła jest jednym z ustawień zasad haseł, które można skonfigurować dla domyślnej zasady hasła domeny lub dla precyzyjnych zasad haseł (FGPP) za pomocą obiektów polityki haseł (PSO). Historia hasła ma na celu zapobieganie recyklingowi haseł, które mogą być już znane przez atakujących lub które mogą być łatwiejsze do odgadnięcia. Domyślnie system Windows zapamiętuje 24 ostatnie hasła, ale można zmienić tę wartość w ustawieniu zasady Enforce password history (Wymuszaj historię haseł).

- złożoność hasła oznacza, że hasło musi zawierać co najmniej trzy spośród następujących czterech typów znaków: wielkie litery, małe litery, cyfry i niealfanumeryczne - symbole takie jak !, #, % lub & i inne np.:



Złożoność hasła jest jednym z ustawień zasad haseł, które można skonfigurować dla domyślnej zasady hasła domeny lub dla precyzyjnych zasad haseł (FGPP) za pomocą obiektów polityki haseł (PSO). Złożoność hasła ma na celu zapobieganie użyciu słabych lub przewidywalnych haseł, które mogą być łatwo złamane przez atakujących.

- wymóg zmiany hasła przy pierwszym logowaniu oznacza, że system wymaga, aby użytkownik ustawił nowe hasło podczas logowania się do konta, które ma ustawione hasło tymczasowe lub które ma wygasłe hasło. Wymóg zmiany hasła przy pierwszym logowaniu jest jednym z ustawień zasad haseł, które można skonfigurować dla domyślnej zasady hasła domeny lub dla precyzyjnych zasad haseł (FGPP) za pomocą obiektów polityki haseł (PSO). Wymóg zmiany hasła przy pierwszym logowaniu ma na celu zapewnić, że użytkownik ma kontrolę nad swoim hasłem i że nikt inny nie może się nim posłużyć. Można włączyć lub wyłączyć ten wymóg dla poszczególnych użytkowników za pomocą pola wyboru User must change password at next logon (Użytkownik musi zmienić hasło przy następnym logowaniu) w oknie właściwości konta użytkownika. Można również użyć polecenia Reset Password (Resetuj hasło) w konsoli Active Directory Users and Computers (ADUC) lub w programie PowerShell, aby wymusić zmianę hasła przy następnym logowaniu.

Użytkownik musi zmieniać hasło co jakiś czas i spełniać pewne wymagania dotyczące hasła.

Te wymagania dotyczą wszystkich użytkowników w domenie, chyba że mają inną politykę hasła (PSO).

Możesz ustawić różne polityki hasła dla różnych użytkowników lub grup za pomocą obiektów PSO.

Obiekty PSO pozwalają określać wymagania dotyczące hasła i blokadę konta dla wybranych użytkowników lub grup.

Możesz tworzyć i przypisywać obiekty PSO za pomocą narzędzi ADAC lub ADSI Edit.

Active Directory nie przechowuje haseł, tylko ich kody skrótu.

Kod skrótu to wynik działania algorytmu na haśle.

Kod skrótu jest niepowtarzalny i nie można z niego odtworzyć hasła.

To zwiększa bezpieczeństwo konta użytkownika.

Niektóre aplikacje chcą czytać hasła użytkowników, ale Active Directory tego nie pozwala.

Można zmienić to ustawieniem Zapisz hasła, korzystając z szyfrowania odwracalnego.

To ustawienie pozwala aplikacjom odszyfrowywać hasła użytkowników.

To ustawienie jest bardzo niebezpieczne dla domeny i domyślnie jest wyłączone.

Lepiej nie używać aplikacji, które chcą czytać hasła użytkowników.

Active Directory sprawdza, czy nowe hasło użytkownika nie jest takie samo jak stare hasła.

Ilość starych haseł, które są sprawdzane, zależy od ustawienia Wymuszaj tworzenie historii haseł.

Domyślnie system Windows sprawdza 24 stare hasła.

Użytkownik nie może zmieniać hasła zbyt często, żeby użyć ponownie stare hasło.

Ustawienie Minimalny okres ważności hasła mówi, jak długo trzeba czekać między zmianami haseł. Domyślnie jest to jeden dzień. To ma zniechęcić użytkownika do powtarzania haseł. Te ustawienia dotyczą tylko użytkownika zmieniającego swoje hasło.

Administrator może zmieniać hasło innego użytkownika bez tych ograniczeń.

Obiekty PSO (Password Settings Object) to specjalne obiekty w Active Directory, które pozwalają na zastosowanie różnych zasad haseł i blokady konta dla różnych użytkowników lub grup. Obiekty PSO są przydatne, gdy chcemy mieć więcej kontroli nad bezpieczeństwem haseł w naszej organizacji.

Obiekty PSO mają następujące cechy:

- Obiekty PSO są tworzone w kontenerze Password Settings Container w domenie Active Directory.
- Obiekty PSO mogą być przypisane do użytkowników lub globalnych grup zabezpieczeń, ale nie do jednostek organizacyjnych (OU).
- Obiekty PSO zawierają wszystkie ustawienia haseł i blokady konta, takie jak minimalna długość hasła, czas wygaśnięcia hasła, historia hasła, próby logowania i czas blokady konta.
- Obiekty PSO są stosowane według zasady pierwszeństwa. Jeśli użytkownik należy do więcej niż jednej grupy zabezpieczeń z przypisanym obiektem PSO, to obowiązuje go obiekt PSO o najniższej wartości atrybutu msDS-PasswordSettingsPrecedence.
- Obiekty PSO są widoczne w atrybucie msDS-ResultantPSO obiektu użytkownika. Możemy sprawdzić ten atrybut, aby dowiedzieć się, jaki obiekt PSO wpływa na danego użytkownika.

W systemach Windows Server 2016, 2019 i 2022 obowiązują następujące zmiany dotyczące polityki haseł i obiektów PSO:

- Minimalna długość hasła może być większa niż 14 znaków. Wcześniej była to maksymalna długość hasła dla systemów Windows Server.
- Można skonfigurować politykę haseł za pomocą usługi Azure AD Password Protection, która pozwala na blokowanie słabych haseł i używanie listy haseł zabronionych.
- Można śledzić aktywność związaną z aktualizacją haseł za pomocą nowych zdarzeń w dzienniku systemu Windows Server 2022.

Polityka haseł w serwerach Windows może być definiowana i zarządzana za pomocą zasady grupy lub za pomocą protokołu LDAP. Polityka haseł w serwerach Windows jest przetwarzana i rozwiązywana przez kontroler domeny systemu Windows pełniący rolę właściciela roli podstawowego kontrolera domeny (PDC) elastycznej operacji pojedynczego wzorca (FSMO) dla domeny systemu Windows. FSMO to skrót od Flexible Single Master Operations, czyli elastycznych operacji pojedynczego wzorca. Jest to zestaw dedykowanych zadań kontrolera domeny (DC), używanych wtedy, gdy standardowe metody transferu i aktualizacji danych są niewystarczające. AD zwykle polega na wielu równorzędnych DC, z których każdy ma kopię bazy danych AD i jest synchronizowany poprzez replikację wielomasterową. Obecnie w systemie Windows istnieje pięć ról FSMO:

- Mistrz schematu
- Mistrz nazewnictwa domen
- Mistrz RID
- Emulator PDC
- Mistrz infrastruktury

Zwykle rolę FSMO przejmuje się tylko wtedy, gdy kontroler domeny zreplikował kontekst nazw (NC), w którym przechowywana jest własność, od momentu uruchomienia usługi katalogowej. Można przenieść lub przejąć rolę FSMO za pomocą narzędzia Windows PowerShell lub Ntdsutil.exe.

W domenie Windows Server 2016, 2019, 2022 polityka haseł jest określona przez zasadę domyślną domeny. Domyślnie przy każdej instalacji usługi Active Directory domyślna Polityka domen ustanawia politykę haseł domen (dla wszystkich użytkowników skonfigurowanych i przechowywanych w usłudze Active Directory). Minimalna długość hasła może być ustawiona na więcej niż 14 znaków, dzięki czemu hasła są trudniejsze do złamania. Wymagania złożoności hasła mogą być zastąpione przez zasady haseł drobnoziarnistych (FGPP), które pozwalają na definiowanie różnych zasad dla różnych grup

użytkowników w domenie. System Windows Server 2022 wprowadził nowe zdarzenia do śledzenia aktywności interakcji z emulatorem kontrolera PDC dotyczących powiadomień dotyczących aktualizacji haseł.

Zasady haseł drobnoziarnistych (FGPP) to technologia firmy Microsoft do kontrolowania zasad haseł, ale nie używa zasad grupowych jako mechanizmu wdrażania. Zamiast tego, FGPP pozwala na tworzenie obiektów zasad haseł (PSO), które są przechowywane w usłudze Active Directory i mogą być stosowane do określonych użytkowników lub grup. PSO zawierają ustawienia takie jak maksymalny wiek hasła, minimalna długość hasła, wymagania złożoności hasła, historia haseł i inne.
FGPP umożliwia definiowanie różnych zasad dla różnych grup użytkowników w domenie, na przykład wymagając silniejszych haseł dla administratorów lub częstszej zmiany haseł dla pracowników zdalnych.

Sposób działania polityki haseł polega na tym, że ten GPO i ustawienia zawarte w tym GPO konfigurują kontrolery domeny (DCs) i znajdujące się na nich bazy danych Active Directory. Zadaniem DCs i znajdujących się na nich baz danych jest filtrowanie każdego hasła, które próbowano zapisać w bazie danych, aby upewnić się, że hasło spełnia ustawienia polityki haseł.

Uwaga: Korzystając z zasad grupy, może istnieć tylko jedna Polityka haseł dla użytkowników domeny. Łączenie i konfigurowanie GPO do OU Nie skonfiguruje polityki haseł inaczej dla użytkowników w tym OU. Ustawienia zasad haseł dotyczą komputerów, a nie kont użytkowników!

Możesz utworzyć nowy GPO, połączyć go z poziomem domeny i nadać mu wyższy priorytet niż domyślna Polityka domeny. Ustawienia w tym nowym GPO (na przykład ustawienie minimalnej długości hasła) zastąpią ustawienia domyślnej Polityki domen ze względu na wyższy priorytet. Pierwszeństwo można ustawić w narzędziu do zarządzania zasadami grupy.

Jeśli chcesz mieć wiele zasad haseł w tej samej domenie, musisz kupić produkt innej firmy lub możesz użyć zasad haseł drobnoziarnistych. Zasady haseł drobnoziarnistych to technologia firmy Microsoft do kontrolowania zasad haseł, ale nie używa zasad grupowych jako mechanizmu wdrażania.

Aby sprawdzić skuteczną politykę haseł domen, oczywiście nie możesz po prostu spojrzeć na domyślną Politykę domen, ponieważ inny GPO powiązany z domeną może mieć inne ustawienia zasad haseł, które zastąpią domyślną Politykę domen. Jak więc poprawnie zweryfikować skuteczną politykę haseł dla użytkowników domeny przechowywanych na kontrolerach domen?

Narzędziem jest secpol.msc i możesz uruchomić to na dowolnym kontrolerze domeny z wiersza polecenia lub przycisku Start / Szukaj programów i plików. Korzystając z secpol.msc, możesz

zweryfikować ze 100% pewnością, jakie są aktualne ustawienia polityki haseł dla użytkowników domeny.

B. Zalety:

a) **Bezpieczeństwo**: Silne hasła minimalizują ryzyko nieautoryzowanego dostępu.

Na przykład:

- Silne hasło powinno zawierać co najmniej 8 znaków, w tym małe i duże litery, cyfry i symbole. Na przykład: !B1nG@2o23.
- Silne hasło powinno być unikalne i niepowiązane z żadnymi osobistymi informacjami, takimi jak imię, data urodzenia czy ulubiony zespół. Na przykład: K0t3k&L1z4k jest lepszym hasłem niż Anna1995.
- Silne hasło powinno być zmieniane co pewien czas, aby utrudnić złamanie go przez hakerów lub złośliwe oprogramowanie. Na przykład: !B1nG@2o23 może być zmienione na !B1nG@2o24 po kilku miesiącach.

Korzyści płynące z używania silnych haseł:

- Zwiększenie poziomu prywatności i ochrony danych osobowych przed nieuprawnionym dostępem lub kradzieżą.
- Zapobieganie włamaniom na konta e-mail, bankowe, społecznościowe lub inne usługi internetowe, które mogą prowadzić do utraty pieniędzy, reputacji lub tożsamości.
- Utrzymanie bezpieczeństwa sieci domowej lub firmowej przed atakami z zewnątrz, które mogą zakłócać działanie urządzeń lub aplikacji.

b) **Ochrona danych**: Polityka haseł pomaga w ochronie danych przechowywanych na serwerach Windows przed nieuprawnionym dostępem lub kradzieżą. Używając silnych i unikalnych haseł, można zapewnić, że tylko uprawnieni użytkownicy mają dostęp do ważnych informacji.
Ponadto, zmieniając hasła co pewien czas, można utrudnić złamanie ich przez hakerów lub złośliwe oprogramowanie. Dodatkowo, korzystając z funkcji ochrony danych dostępnych w systemach Windows Server 2016, 2019 i 2022, takich jak Windows Admin Center, Hybrid Cloud, ESET File Security i Microsoft Defender for Endpoint, można zwiększyć poziom bezpieczeństwa i ciągłości działania serwerów.

c) **Zgodność**: Polityka haseł wspomaga spełnianie regulacji dotyczących bezpieczeństwa danych, takich jak RODO, PCI DSS. Ustalając minimalną długość, złożoność i okres ważności haseł, można zapewnić, że dane są chronione zgodnie z wymogami prawnymi i branżowymi. Ponadto, stosując zasadę najmniejszych uprawnień i audytując aktywność użytkowników, można zapobiec nadużyciom i naruszeniom danych. Dodatkowo, korzystając z funkcji ochrony danych dostępnych w systemach Windows Server 2016, 2019 i 2022, takich jak Windows Admin Center, Hybrid Cloud, ESET File Security i Microsoft Defender for Endpoint, można łatwiej zarządzać i monitorować zgodność serwerów.

RODO to skrót od Ogólnego rozporządzenia o ochronie danych (angGeneral Data Protection Regulation, GDPR), które jest unijnym aktem prawnym, zawierającym przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływie takich danych. RODO obowiązuje od 25 maja 2018 roku i ma na celu wzmocnić prawa i wolności osób, których dane są przetwarzane, oraz ujednolicić zasady ochrony danych w całej Unii Europejskiej. RODO wprowadza m.in. takie zasady jak:

- Zgodność: dane osobowe muszą być przetwarzane zgodnie z prawem, uczciwie i przejrzyście
- Minimalizacja: dane osobowe muszą być adekwatne, stosowne i ograniczone do tego, co niezbędne
- Celowość: dane osobowe muszą być zbierane do określonych, wyraźnych i prawnie uzasadnionych celów
- Dokładność: dane osobowe muszą być dokładne i aktualne
- Ograniczenie przechowywania: dane osobowe muszą być przechowywane nie dłużej, niż jest to konieczne
- Integralność i poufność: dane osobowe muszą być chronione przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem, utratą, zniszczeniem lub uszkodzeniem

PCI DSS to skrót od Payment Card Industry Data Security Standard, czyli normy bezpieczeństwa danych w branży kart płatniczych. Jest to norma wydana przez Payment Card Industry Security Standards Council, która ma na celu zapewnić wysoki i spójny poziom bezpieczeństwa we wszystkich środowiskach, w których przetwarzane są dane posiadaczy kart płatniczych. Stosowanie tej normy jest wymagane przez główne marki kart, takie jak Visa, Mastercard, American Express czy Discover. Norma PCI DSS składa się z 12 wymagań podzielonych na sześć obszarów kontrolnych, takich jak:

- Budowanie i utrzymywanie bezpiecznej sieci i systemów

- Ochrona danych posiadaczy kart
- Utrzymywanie programu zarządzania podatnościami
- Implementacja silnych środków kontroli dostępu
- Monitorowanie i testowanie regularnie sieci
- Utrzymywanie polityki bezpieczeństwa informacji

C. **Elementy:**

a) **Silne hasła**: Wymuszanie używania haseł zawierających różne typy znaków.

Silne hasła to takie, które zawierają różne typy znaków, takie jak litery, cyfry, symbole i wielkie litery. Silne hasła są trudniejsze do odgadnięcia lub złamania przez osoby nieuprawnione lub złośliwe oprogramowanie. W kontekście polityki haseł Windows Server silne hasła można wymusić za pomocą dyrektyw zabezpieczeń lokalnych lub zasad grupy. Dyrektywy zabezpieczeń lokalnych pozwalają na ustawienie minimalnej długości hasła, historii hasła, złożoności hasła i wieku hasła dla kont lokalnych na serwerze. Zasady grupy pozwalają na ustawienie tych samych parametrów dla kont domenowych w całej domenie Active Directory. Wymuszanie minimalnej długości hasła co najmniej 15 znaków jest obsługiwane w programie Windows Server, w wersji 2004 oraz w nowszych wersjach Windows. Aby zmienić hasło użytkownika usługi Windows Active Directory i LDS za pośrednictwem protokołu LDAP, można użyć narzędzia ldp.exe lub ldifde.exe.

b) **Okresowe zmiany haseł**: Wymóg regularnej zmiany haseł w celu zapobieżenia atakom.

Okresowe zmiany haseł to wymóg regularnej zmiany haseł w celu zapobieżenia atakom, takim jak złamanie hasła, przechwycenie hasła lub ujawnienie hasła. Okresowe zmiany haseł zmuszają użytkowników do tworzenia nowych haseł co pewien czas, co utrudnia potencjalnym włamywaczom uzyskanie dostępu do kont. W kontekście polityki haseł Windows Server, okresowe zmiany haseł można wymusić za pomocą dyrektyw zabezpieczeń lokalnych lub zasad grupy.
Dyrektywy zabezpieczeń lokalnych pozwalają na ustawienie maksymalnego wieku hasła dla kont lokalnych na serwerze. Zasady grupy pozwalają na ustawienie tego samego parametru dla kont domenowych w całej domenie Active Directory. Maksymalny wiek hasła określa liczbę dni, po których użytkownik musi zmienić hasło. Domyślnie jest to 42 dni, ale można go zmienić według własnych potrzeb. Aby zmienić hasło użytkownika usługi Windows Active Directory i LDS za pośrednictwem protokołu LDAP, można użyć narzędzia ldp.exe lub ldifde.exe.

c) **Blokady po nieudanych próbach**: Chronienie przed atakami typu "brute force".

Blokady po nieudanych próbach to funkcja, która chroni przed atakami typu “brute force”, polegającymi na wielokrotnym próbowaniu różnych haseł, aż do znalezienia tego właściwego. Blokady po nieudanych próbach uniemożliwiają lub ograniczają dostęp do konta po określonej liczbie nieudanych prób logowania. W kontekście polityki haseł Windows Server, blokady po nieudanych próbach można wymusić za pomocą dyrektyw zabezpieczeń lokalnych lub zasad grupy. Dyrektywy zabezpieczeń lokalnych pozwalają na ustawienie progu blokady konta, czasu trwania blokady konta i czasu resetowania licznika blokady konta dla kont lokalnych na serwerze. Zasady grupy pozwalają na ustawienie tych samych parametrów dla kont domenowych w całej domenie Active Directory. Próg blokady konta określa liczbę nieudanych prób logowania, po których konto zostaje zablokowane. Domyślnie jest to **0**, co oznacza, że **blokada konta jest wyłączona**, ale można go zmienić według własnych potrzeb. Czas trwania blokady konta określa czas, przez który konto pozostaje zablokowane. Domyślnie to nie określono, co oznacza, że konto musi być odblokowane przez administratora, ale można go zmienić według własnych potrzeb.
Czas resetowania licznika blokady konta określa czas, po którym licznik nieudanych prób logowania jest zerowany. Domyślnie jest to 30 minut, ale można go zmienić według własnych potrzeb.

d) **Historia haseł**: Zapobieganie powtarzaniu tych samych haseł.

Historia haseł to funkcja, która zapobiega powtarzaniu tych samych haseł przez użytkowników. Historia haseł zapamiętuje poprzednie hasła użytkownika i uniemożliwia ich ponowne użycie.
W kontekście polityki haseł Windows Server 2016, 2019, 2022, historię haseł można wymusić za pomocą dyrektyw zabezpieczeń lokalnych lub zasad grupy. Dyrektywy zabezpieczeń lokalnych pozwalają na ustawienie długości historii haseł dla kont lokalnych na serwerze. Zasady grupy pozwalają na ustawienie tego samego parametru dla kont domenowych w całej domenie Active Directory. Długość historii haseł określa liczbę poprzednich haseł, które są zapamiętywane i nie mogą być ponownie użyte. Domyślnie jest to 24, ale można go zmienić według własnych potrzeb.

D. Konfigurowanie zasad haseł i zasad blokady konta

W Windows Server 2016, 2019, 2022 polega to na użyciu narzędzia Zarządzanie zasadami grupy (GPMC), które umożliwia tworzenie, edytowanie i stosowanie obiektów zasad grupy (GPO) do jednostek organizacyjnych (OU) w domenie.

Zasady haseł i zasady blokady konta są częścią zasad konta w GPO i dotyczą wszystkich użytkowników w OU.

Zasady haseł określają ustawienia takie jak minimalna długość hasła, maksymalny wiek hasła, wymagania złożoności hasła, historia haseł i inne.

Zasady blokady konta określają ustawienia takie jak próg blokady konta, czas trwania blokady konta, czas resetowania licznika blokady konta i inne.

Aby skonfigurować te zasady, należy otworzyć GPMC, wybrać odpowiedni GPO, kliknąć prawym przyciskiem myszy i wybrać opcję Edytuj. Należy przejść do Konfiguracja komputera > Zasady > Ustawienia systemu Windows > Ustawienia zabezpieczeń > Zasady konta i wybrać Zasady haseł lub Zasady blokady konta. Tam można zmienić ustawienia według własnych potrzeb i zastosować zmiany.

Pierwszeństwo obiektów PSO określa, która zasada hasła będzie obowiązywać, gdy użytkownik lub grupa jest powiązany z więcej niż jednym PSO. Pierwszeństwo PSO jest określane przez atrybut msDS-PasswordSettingsPrecedence w obiekcie PSO. Im niższa jest wartość tego atrybutu, tym wyższe jest pierwszeństwo PSO. Jeśli użytkownik lub grupa nie jest powiązany z żadnym PSO, obowiązuje domyślna zasada hasła domeny. Wynikowy obiekt PSO (RSOP) to efektywna zasada hasła, która wynika z zastosowania pierwszeństwa PSO do użytkownika lub grupy.

Aby sprawdzić wynikowy zestaw zasad RSOP dla użytkownika lub grupy, można użyć narzędzia:

- Wynikowy zestaw zasad (RSOP), który jest dostępny jako plik Rsop.msc. Aby użyć tego narzędzia, należy kliknąć przycisk Start, kliknąć przycisk Uruchom, wpisać mmc w polu Otwórz, a następnie kliknąć przycisk OK. Następnie należy dodać moduł RSOP do konsoli MMC i wybrać użytkownika lub grupę, dla którego chcemy sprawdzić RSOP.
Można też użyć polecenia Get-ADUserResultantPasswordPolicy w PowerShellu, które zwraca RSOP dla użytkownika na podstawie atrybutu msDS-ResultantPSO.
- Active Directory Administrative Center (ADAC) i wybrać opcję Zobacz wynikowy obiekt ustawień haseł w menu kontekstowym.

Podsumowanie: Zarządzanie zasadami grup oraz polityką haseł w serwerach Windows 2016, 2019 i 2022 ma kluczowe znaczenie dla organizacji, bezpieczeństwa i efektywności. Poprzez konfigurację odpowiednich zasad grup oraz polityk haseł, administratorzy mogą skutecznie zarządzać dostępem, minimalizować ryzyko ataków i chronić dane. Te teoretyczne koncepty stanowią podstawę dla praktycznych działań w środowiskach serwerowych.