Temat: Delegowanie i zabezpieczenia obiektów ADDS. Tworzenie profili kont użytkowników ADDS.

Cel Ogólny lekcji: Celem ogólnym lekcji jest zrozumienie koncepcji delegowania i zabezpieczeń obiektów w kontekście usługi katalogowej Active Directory oraz umiejętność tworzenia i konfigurowania profili kont użytkowników w środowisku Active Directory.

Cele szczegółowe:

Na podstawie powyższego tekstu, cele szczegółowe lekcji mogą być zdefiniowane następująco:

1. **Delegowanie i Zabezpieczenia Obiektów w Active Directory:**

- Wyjaśnienie, czym jest Active Directory i jego rola w zarządzaniu zasobami sieciowymi.
- Zrozumienie pojęcia delegacji w kontekście zarządzania obiektami w AD.
- Omówienie korzyści z delegowania uprawnień w celu zrównoważonego zarządzania.
- Zrozumienie poziomów, na których można przeprowadzać delegację (drzewo katalogu, domena, jednostka organizacyjna).
- Wyjaśnienie procesu delegacji w AD, obejmującego wybór obiektów, określenie uprawnień i obszaru działania.
- Przykłady typowych uprawnień, które można przekazywać poprzez delegację.

2. **Tworzenie Profili Kont Użytkowników w Active Directory:**

- Przypomnienie podstawowych wiadomości związanych z profilami kont użytkowników z klasy pierwszej.
- Zrozumienie roli profili użytkowników w dostosowaniu środowiska pracy użytkownika na komputerze.
- Wyjaśnienie różnych typów profili użytkowników: lokalne, mobilne, obowiązkowe, tymczasowe.
- Zrozumienie składników profilu użytkownika: gałąź rejestru i zestaw folderów profilu.
- Omówienie korzyści wynikających z korzystania z różnych typów profili użytkowników.
- Zrozumienie procesu tworzenia mobilnych profili użytkowników oraz ich zalet, takich jak automatyczna dostępność zasobów i uproszczona wymiana komputera.

3. **Wdrażanie Profili Użytkowników Mobilnych:**

- Przedstawienie kroków potrzebnych do wdrożenia profili użytkowników mobilnych w środowisku sieciowym.
- Omówienie konieczności stworzenia grupy zabezpieczeń dla użytkowników mobilnych.

- Zrozumienie procesu tworzenia udziału pliku na serwerze dla przechowywania profili użytkowników mobilnych.
- Wyjaśnienie roli obiektu zasad grupy w konfiguracji profili użytkowników mobilnych.
- Omówienie ustawień profili użytkowników mobilnych, włączając na koncie użytkownika w AD DS oraz komputerze w zasadach grupy.

4. Zabezpieczenia i Optymalizacje:

- Wyjaśnienie, dlaczego zabezpieczenia profili użytkowników są ważne w kontekście bezpieczeństwa infrastruktury.
- Omówienie opcji optymalizacji przy pierwszym logowaniu, włączając w to przyspieszenie logowania użytkowników.
- Przedstawienie możliwości usuwania niepotrzebnych aplikacji z obrazu systemu Windows 10 w celu optymalizacji profili użytkowników.

5. Teoretyczne przykłady praktycznego wykorzystania profili użytkowników:

- Wyjaśnienie, jak ustawić domyślny układ pulpitu dla komputerów z Windows 10.
- Omówienie funkcji podstawowego komputera i sposobów jej implementacji.
- Wskazówki dotyczące wdrożenia i monitorowania profili użytkowników mobilnych w praktyce.

Podsumowanie:

Cele ogólne i szczegółowe lekcji mają na celu dostarczenie uczniom wiedzy na temat delegowania i zabezpieczeń obiektów w Active Directory oraz umiejętności tworzenia i konfigurowania

Delegowanie i Zabezpieczenia Obiektów w Active Directory:

Active Directory (AD) to usługa katalogowa opracowana przez firmę Microsoft, która umożliwia zarządzanie zasobami sieciowymi, takimi jak użytkownicy, grupy, komputery i inne obiekty. Delegowanie i zabezpieczenia obiektów AD odnoszą się do zarządzania dostępem do tych obiektów oraz przekazywania pewnych uprawnień do zarządzania nimi.

1. **Delegowanie w Active Directory:**

Delegowanie polega na przekazywaniu części uprawnień administracyjnych do zarządzania obiektami AD innym użytkownikom lub grupom. Pozwala to na rozłożenie obciążenia administracyjnego oraz umożliwia bardziej zrównoważone zarządzanie. Delegowanie może być przeprowadzane na różnych poziomach, w tym na poziomie drzewa katalogu, domeny lub jednostki organizacyjnej (OU).

Delegacja w AD obejmuje następujące kroki:

- Wybór obiektów do delegacji.
- Określenie uprawnień, które zostaną udzielone delegowanym użytkownikom.
- Ustalenie obszaru, na którym będą mogli działać delegowani użytkownicy.

Przykładowe uprawnienia, które można przekazać poprzez delegację, to dodawanie i usuwanie użytkowników do/ze specyficznych grup, zarządzanie hasłami, odblokowywanie kont, itp.

2. **Tworzenie profili kont użytkowników**

Ogólne przypomnienie wiadomości z klasy pierwszej:
Podstawy dot. profili kont użytkowników dotyczące systemu lokalnego (Windows 10) były w klasie pierwszej.
Poniżej przedstawiłem elementy przypomnienia rozszerzonego o kolejne zagadnienia.

Profil użytkownika to zbiór ustawień i preferencji, które określają wygląd i sposób pracy z komputerem. Profil użytkownika jest tworzony przy pierwszym logowaniu do komputera i przechowywany lokalnie lub zdalnie. Podczas kolejnych logowań system wczytuje profil użytkownika i dostosowuje środowisko do niego.

Tworzenie profili kont użytkowników w AD odnosi się do konfigurowania ustawień i dostępów dla konkretnych użytkowników w kontekście ich dostępu do zasobów i działań w sieci.

Typy profilów użytkowników to:

Lokalne: Tworzone na komputerze, przechowywane na dysku, zmiany dotyczą tylko tego komputera i użytkownika.

Mobilne: Kopia lokalnego profilu na serwerze, pobierana na każdy komputer w sieci, zmiany synchronizowane z serwerem, zaleta: jeden profil na wiele komputerów.

Obowiązkowe: Ustalone przez administratora, nie można zmieniać ustawień pulpitu, tylko administrator może zmieniać profil.

Tymczasowe: Wydawane przy błędzie ładowania profilu, usuwane po wylogowaniu, zmiany tracone.

Można to uprościć tak:

Lokalne: Na jednym komputerze.

Mobilne: Na wielu komputerach w sieci.

Obowiązkowe: Bez zmian ustawień.

Tymczasowe: Przy błędzie, bez zapisu zmian.

Profil użytkownika składa się z:

Gałąź rejestru: Plik NTuser.dat, ładowany podczas logowania, przechowuje ustawienia użytkownika.

Zestaw folderów profilu: Przechowywane w katalogu Profile, zawierają pliki użytkownika, np. dokumenty, pliki konfiguracyjne, tło pulpitu.

Profile użytkowników zapewniają:

Zachowanie ustawień: Użytkownik ma te same ustawienia po każdym logowaniu.

Personalizację pulpitu: Użytkownik ma własny pulpit, menu Start, folder Dokumenty itp. po zalogowaniu.

Ochronę danych: Ustawienia i pliki użytkownika są prywatne i niezależne od innych użytkowników.

Mobilne profile użytkowników to:

Automatyczna dostępność zasobów: Użytkownik ma swój profil na każdym komputerze w sieci.

Uproszczona wymiana komputera i kopia zapasowa: Użytkownik nie traci swojego profilu, gdy zmienia komputer.

Załadowanie i zwolnienie profilu: Użytkownik musi użyć funkcji LoadUserProfile i UnloadUserProfile, aby załadować i zwolnić swój profil.

Obowiązkowy profil użytkownika to:

Profil mobilny z ustawieniami administratora: Użytkownik nie może zapisać zmian w swoim profilu.

Profil tylko do odczytu z rozszerzeniem .man: Użytkownik musi mieć plik NTuser.man w swoim folderze profilu.

Superobowiązkowy profil z folderem .man: Użytkownik musi mieć folder profilu zakończony na .man i nie może się zalogować bez serwera.

Tymczasowy profil użytkownika to:

Profil zastępczy przy błędzie: Użytkownik nie ma dostępu do swoich plików i ustawień.

Profil usuwany po sesji: Użytkownik traci zmiany wprowadzone w profilu.

Profil dostępny od Windows 2000: Użytkownik nie może używać profilu tymczasowego w starszych systemach.

W ramach tworzenia profili kont użytkowników można określić:

Ustawienia logowania: Dotyczy to ustawień takich jak ograniczenia dostępu do pewnych godzin, wymuszanie zmiany hasła przy pierwszym logowaniu, ustawienia zabezpieczeń, itp.

Przypisywanie grup: Określenie do których grup użytkownik będzie przynależał, co wpływa na jego dostęp do zasobów i aplikacji.

Uprawnienia: Można skonfigurować uprawnienia dostępu do konkretnych zasobów sieciowych, takich jak foldery i drukarki.

Polityki bezpieczeństwa: Dotyczy to ustawień związanych z hasłami, zasadami haseł, blokadami konta po nieudanych próbach logowania, itp.

Skrypty Logowania: Umożliwiają wykonanie określonych działań lub konfiguracji przy logowaniu lub wylogowaniu użytkownika.

Wszystkie te aspekty pomagają w efektywnym zarządzaniu zasobami i dostępem w środowisku Active Directory oraz w zabezpieczaniu infrastruktury przed niepożądanym dostępem i zagrożeniami.

3. Wdrażanie profilów użytkowników mobilnych

Roamingowy profil użytkownika to:

Profil przenoszony na serwer: Użytkownik ma ten sam profil na różnych komputerach.

Profil wymagający procesora x64 lub x86: Użytkownik nie może używać profilu roamingowego na Windows RT.

Profil zależny od wersji systemu: Użytkownik może mieć problemy z profilem roamingowym między różnymi wersjami systemu Windows.

Roamingowe profile użytkowników mają następujące wymagania dotyczące oprogramowania:

Przekierowanie folderów przed profilami roamingowymi: Użytkownik musi przekierować foldery profilu na serwer, aby zmniejszyć rozmiar profilu roamingowego.

Uprawnienia administratora: Użytkownik musi być administratorem domeny, przedsiębiorstwa lub twórcą zasad grupy, aby zarządzać profilami roamingowymi.

Kompatybilność systemu operacyjnego: Użytkownik musi mieć system Windows 10 lub Windows Serwer 2016 lub nowszy, aby uniknąć problemów z wersjami profilów roamingowych.

Przyłączenie do domeny: Użytkownik musi być przyłączony do domeny Active Directory, którą zarządzasz.

Dostępność serwera: Użytkownik musi mieć dostęp do serwera plików i zarządzania zasadami grupy.

Udział plików używany przez roamingowe profile użytkowników musi spełniać następujące wymagania:

Jeden cel DFS: Użytkownik musi mieć dostęp do tego samego folderu na serwerze, aby uniknąć konfliktów edycji.

Serwer źródłowy DFS: Użytkownik musi mieć dostęp do serwera, z którego replikowane są dane, aby uniknąć konfliktów edycji.

Wyłączona ciągła dostępność: Użytkownik musi wyłączyć tę funkcję na udziale plików klastrowanym, aby uniknąć problemów z wydajnością.

Podstawowa obsługa komputera: Użytkownik musi mieć dodatkowe wymagania dotyczące komputera klienckiego i schematu Active Directory, aby korzystać z tej funkcji.

Użytkownik nie będzie miał tego samego układu menu Start na różnych komputerach lub serwerach, jeśli używa profilu użytkownika mobilnego. Aby obejść ten problem, użytkownik może zrobić jedno z dwóch:

- **Określić układ początkowy**: Użytkownik może ustawić układ menu Start, który będzie stosowany dla wszystkich nowych profili.
- **Użyć dysków profilu użytkownika**: Użytkownik może użyć tej funkcji, aby zachować ustawienia menu Start na serwerach Host sesji usług pulpitu zdalnego lub serwerach VDI.

Host sesji usług pulpitu zdalnego to serwer, który umożliwia użytkownikom zdalny dostęp do aplikacji i pulpitu na systemie Windows Server. **Serwer VDI to** serwer, który umożliwia użytkownikom zdalny dostęp do wirtualnych maszyn z systemem Windows 10 lub innych systemów operacyjnych. Oba typy serwerów wymagają licencji dostępu klienta usług pulpitu zdalnego (CAL) i mogą być zarządzane przez usługę Azure Virtual Desktop.

Jeśli użytkownik chce używać profilu użytkownika mobilnego w wielu wersjach systemu Windows, zalecamy podjęcie następujących działań:

- **Przechowywać osobne wersje profili**: Użytkownik może skonfigurować system Windows, aby utworzył osobny profil dla każdej wersji systemu operacyjnego. Pomaga to zapobiegać uszkodzeniu profilu.
- **Przekierować folder**: Użytkownik może przechowywać pliki użytkownika, takie jak dokumenty i obrazy, poza profilem użytkownika. Dzięki temu te same pliki będą dostępne w różnych wersjach systemu operacyjnego. Utrzymuje to również małe profile i szybkie logowanie.

Wędrowanie profilu użytkownika mobilnego między różnymi wersjami systemu Windows Server nie jest obsługiwane z powodu niezgodności w ich wersjach profilowych. Dlatego zaleca się używanie przechowywania wersji profilów, które umożliwia utrzymywanie osobnych kopii profilu dla każdej wersji systemu. Aby zachować dane użytkowników, można użyć Przekierowania folderu.

W Windows 10, Windows Server 2016 i nowszych wersjach systemu Windows przechowywanie wersji profilów jest domyślnie włączone. Nie musisz instalować żadnych aktualizacji ani tworzyć klucza rejestru. Wystarczy, że uruchomisz ponownie komputery.

Jeśli chcesz używać mobilnych profili użytkowników, musisz stworzyć grupę zabezpieczeń dla nich. W zależności od tego, jakie masz środowisko, możesz dodać do grupy użytkowników i/lub komputery.

Jeśli potrzebujesz udziału plików dla mobilnych profili użytkowników (nie mylić z udziałem dla przekierowanych folderów), zrób tak na serwerze z systemem Windows Server. Ustaw odpowiednie uprawnienia dla konta System, Administratorzy, Twórca i grupy zabezpieczeń użytkowników mobilnych. Usuń inne grupy i konta z uprawnień.

Jeśli potrzebujesz obiektu zasad grupy dla mobilnych profili użytkowników, zrób pusty obiekt i skonfiguruj ustawienia według potrzeb. Ten obiekt zasad grupy pozwala na dostosowanie mobilnych profili użytkowników (np. komputer podstawowy) i włączanie ich na komputerach w środowiskach wirtualnych lub zdalnych.

Jeśli chcesz używać mobilnych profili użytkowników na kontach użytkowników, ustaw je w usłudze Active Directory.
Jeśli chcesz używać mobilnych profili użytkowników na komputerach, zrób to w zasadach grupy.
Uwaga: zasady grupy mają pierwszeństwo nad usługą Active Directory.
W profilu użytkownika podaj ścieżkę do udziału plików z profilem mobilnym.
Użyj %username% jako zmiennej. Na przykład: \fs1.corp.contoso.com\User Profiles$%username%

Jeśli chcesz używać obowiązkowego profilu mobilnego, podaj ścieżkę do pliku NTuser.man.
Na przykład: \fs1.corp.contoso.com\User Profiles$\default
Domyślnie aplikacje oparte na Windows Store są dozwolone z profilami mobilnymi. Ale nie z profilami specjalnymi, które się nie zapisują po wylogowaniu.

Jeśli chcesz używać mobilnych profili użytkowników na komputerach, zrób to w zasadach grupy.
To działa na systemach Windows 8.1 i nowszych oraz Windows Server 2008 i nowszych.
Jeśli chcesz używać mobilnych profili użytkowników na kontach użytkowników, zrób to w usłudze Active Directory.
Uwaga: zasady grupy mają pierwszeństwo nad usługą Active Directory.
W zasadach grupy podaj ścieżkę do udziału plików z profilem mobilnym.
Użyj %username% jako zmiennej. Na przykład: \fs1.corp.contoso.com\User Profiles$%username%
Jeśli chcesz używać obowiązkowego profilu mobilnego, podaj ścieżkę do pliku NTuser.man.
Na przykład: \fs1.corp.contoso.com\User Profiles$\default

Jeśli chcesz ustawić określony układ menu Start na komputerach z Windows 10, zrób to w zasadach grupy. To działa na systemach Windows 10 1607 i nowszych z aktualizacją KB4013429 lub nowszą. Musisz też wykonać te czynności: Utwórz plik XML z układem menu Start. Możesz zablokować całe menu Start lub tylko niektóre grupy kafelków. Zobacz, jak to zrobić tutaj.

Zastosuj plik XML do obiektu zasad grupy dla mobilnych profili użytkowników.

Aby zastosować plik XML do obiektu zasad grupy dla mobilnych profili użytkowników, wykonaj następujące kroki:

1. Otwórz Edytor zasad grupy i przejdź do Konfiguracja użytkownika > Szablony administracyjne > Menu Start i pasek zadań.
2. Kliknij dwukrotnie pozycję Określ układ menu Start.
3. Wybierz opcję Włączone i kliknij przycisk Przeglądaj, aby wybrać plik XML z układem menu Start.
4. Kliknij przycisk OK, aby zastosować ustawienie i zamknąć okno dialogowe.
5. Zamknij Edytor zasad grupy i zaktualizuj zasady grupy na komputerach docelowych.

Ustaw wartość rejestru SpecialRoamingOverrideAllowed na 1 na komputerach z Windows 10.

Aby ustawić wartość rejestru SpecialRoamingOverrideAllowed na 1 na komputerach z Windows 10, wykonaj następujące kroki:

1. Otwórz Edytor rejestru i przejdź do klucza HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer.

2. Kliknij prawym przyciskiem myszy na pustym obszarze w prawym okienku i wybierz opcję Nowy > Wartość DWORD (32-bitowa).
3. Nadaj wartości nazwę SpecialRoamingOverrideAllowed i kliknij dwukrotnie na niej, aby ją edytować.
4. W polu Dane wartości wpisz 1 i kliknij przycisk OK.
5. Zamknij Edytor rejestru i zrestartuj komputer, aby zastosować zmianę.

Jeśli chcesz przyspieszyć logowanie użytkowników, możesz zrobić dwie rzeczy: Włącz optymalizacje przy pierwszym logowaniu w zasadach grupy. Zobacz, jak to zrobić tutaj .
Usuń zbędne aplikacje z obrazu Windows 10, który używasz do instalowania systemu na komputerach. Nie musisz tego robić na obrazach serwera.

Jeśli chcesz usunąć niepotrzebne aplikacje z obrazu Windows 10, możesz użyć polecenia Remove-AppxProvisionedPackage w PowerShell. Możesz też użyć zasady grupy, aby odinstalować aplikacje z komputerów już wdrożonych. Oto lista aplikacji, które możesz usunąć:

Microsoft.windowscommunicationsapps

Microsoft.BingWeather

Microsoft.DesktopAppInstaller

Microsoft.Getstarted

Microsoft.Windows.Photos

Microsoft.WindowsCamera

Microsoft.WindowsFeedbackHub

Microsoft.WindowsStore

Microsoft.XboxApp

Microsoft.XboxIdentityProvider

Microsoft.ZuneMusic

Jeśli chcesz używać mobilnych profili użytkowników, musisz włączyć obiekt zasad grupy (GPO), który je konfiguruje. Możesz też ustawić komputery podstawowe dla użytkowników, aby ograniczyć kopiowanie danych. Oto jak włączyć GPO:

- Otwórz Zarządzanie zasadami grupy.

- Kliknij prawym przyciskiem myszy GPO, który utworzyłeś.
- Wybierz Link Enabled. Zaznacz pole wyboru.

Możesz znaleźć więcej informacji na tych stronach.

Aby sprawdzić, czy mobilne profile użytkowników działają poprawnie, zaloguj się na komputerze z kontem z włączonym profilem mobilnym. Upewnij się, że komputer jest podstawowy lub ma zasadę grupy dla profilu mobilnego. Następnie zobacz, czy profil jest przenoszony. Oto jak to zrobić:

- Zaloguj się na komputerze podstawowym lub z zasadą grupy dla profilu mobilnego.
- Jeśli już się logowałeś na tym komputerze, wpisz w PowerShell: GpUpdate /Force
- Aby sprawdzić, czy profil jest przenoszony, otwórz Panel sterowania > System i zabezpieczenia > System > Zaawansowane ustawienia systemu > Ustawienia w Profilach użytkowników. Zobacz, czy w Typ jest Roaming.

Witaj, to jest Bing. Chętnie pomogę Ci z tym tekstem. Oto uproszczona wersja:

Dodatek A: Jak wdrożyć profile użytkowników mobilnych

1. Przygotuj domenę
   - Podłącz komputery do domeny
   - Ustaw osobne profile dla różnych systemów operacyjnych
   - Stwórz konta użytkowników
   - (Opcjonalnie) Przenieś foldery użytkowników na serwer
2. Stwórz grupę zabezpieczeń dla użytkowników mobilnych
   - Nazwa grupy:
   - Członkowie:
3. Stwórz udział pliku na serwerze dla profili użytkowników mobilnych
   - Nazwa udziału pliku:
4. Stwórz obiekt zasad grupy dla użytkowników mobilnych
   - Nazwa obiektu zasad grupy:
5. Ustaw profile użytkowników mobilnych
6. Włącz profile użytkowników mobilnych
   - Włączone na kontach użytkowników w AD DS?
   - Włączone na kontach komputerowych w zasadach grupy?
7. (Opcjonalnie) Ustaw domyślny układ pulpitu dla komputerów z Windows 10
8. (Opcjonalnie) Włącz funkcję podstawowego komputera

- Przypisz podstawowe komputery do użytkowników
- Lokalizacja mapowania użytkownika i podstawowego komputera:
- (Opcjonalnie) Włącz funkcję podstawowego komputera dla przeniesionych folderów
- Na poziomie komputera czy użytkownika?
- (Opcjonalnie) Włącz funkcję podstawowego komputera dla profili użytkowników mobilnych

9. Włącz obiekt zasad grupy dla profili użytkowników mobilnych
10. Sprawdź działanie profili użytkowników mobilnych

Powyższe informacje są aktualne dla systemów Windows Server 2016, 2019 i 2022.

Dodatek B: Wersje profili użytkowników

Każdy profil ma swoją wersję, która zależy od wersji systemu Windows. Niektóre wersje systemu Windows mają taką samą wersję profilu, a niektóre mają różne. Microsoft zmienia wersję profilu tylko gdy jest to potrzebne.

Poniżej pokazano, gdzie są zapisywane profile użytkowników mobilnych w różnych wersjach systemu Windows.

Wersja systemu operacyjnego Miejsce zapisu profilu użytkownika mobilnego

Windows XP i Windows Server 2003 \<nazwa_serwera><nazwa_udziału><nazwa_użytkownika>
Windows Vista i Windows Server 2008 \<nazwa_serwera><nazwa_udziału><nazwa_użytkownika>.V2
Windows 7 i Windows Server 2008 R2 \<nazwa_serwera><nazwa_udziału><nazwa_użytkownika>.V2
Windows 8 i Windows Server 2012 <nazwa_serwera><nazwa_udziału><nazwa_użytkownika>.V3(jeśli zainstalowano aktualizację i zmieniono rejestr) \<nazwa_serwera> <nazwa_udziału> <nazwa_użytkownika>.V2(jeśli nie zainstalowano aktualizacji lub nie zmieniono rejestru)

Windows 8.1 i Windows Server 2012 R2 \<nazwa_serwera> <nazwa_udziału> <nazwa_użytkownika> .V4(jeśli zainstalowano aktualizację i zmieniono rejestr) \<nazwa_serwera> <nazwa_udziału> <nazwa_użytkownika>.V2(jeśli nie zainstalowano aktualizacji lub nie zmieniono rejestru)

Windows 10 \<nazwa_serwera><nazwa_udziału><nazwa_użytkownika>.V5

Windows 10, wersja 1703 i wersja 1607 \<nazwa_serwera><nazwa_udziału><nazwa_użytkownika>.V6
Windows 10, wersja 1803 i nowsze oraz Windows Server 2016, 2019 i 2022 \<nazwa_serwera> <nazwa_udziału><nazwa_użytkownika>.V6

Powyższe informacje są aktualne dla systemów Windows Server 2016, 2019 i 2022 oraz odpowiadających im systemów klienckich.

Podczas tej lekcji uczestnicy dowiedzieli się, jak skutecznie zarządzać dostępem do zasobów sieciowych poprzez delegowanie uprawnień, a także jak tworzyć i konfigurować profile kont użytkowników, aby zapewnić personalizację, dostęp do zasobów i zabezpieczenia.
Leżące u podstaw zagadnienia pozwalają na efektywne zarządzanie infrastrukturą w środowisku Active Directory oraz zwiększenie bezpieczeństwa w organizacji.