4. Ćwiczenia w grupach: Podziel uczestników na grupy i przydziel im zadania związane z różnymi aspektami Active Directory. Poproś każdą grupę o przygotowanie krótkiej prezentacji lub raportu na temat swojego zagadnienia.

Przykłady ćwiczeń w grupach związanych z różnymi aspektami Active Directory:

Ćwiczenia w grupach: Aspekty Active Directory

Podziel uczestników na kilka grup, a następnie przydziel każdej grupie jedno z poniższych zadań. Poproś każdą grupę o przygotowanie krótkiej prezentacji lub raportu na temat swojego zagadnienia. Po zakończeniu prezentacji grupy mogą zadawać sobie nawzajem pytania lub omawiać aspekty innych grup.

Grupa 1: Hierarchiczna struktura Active Directory

- Omówienie hierarchicznej struktury jednostek organizacyjnych (OU) w Active Directory.
- Przedstawienie korzyści wynikających z właściwego ułożenia OU w kontekście zarządzania.

Grupa 2: Delegowanie kontroli w Active Directory

- Wyjaśnienie procesu delegowania uprawnień w ramach Active Directory.
- Przykłady scenariuszy, w których delegowanie uprawnień jest ważne, oraz jakie uprawnienia można delegować.

Grupa 3: Rola DNS w Active Directory

- Wyjaśnienie, jak DNS (Domain Name System) odgrywa kluczową rolę w infrastrukturze Active Directory.
- Przedstawienie, dlaczego poprawna konfiguracja DNS jest istotna dla działania AD.

Grupa 4: Grupy zabezpieczeń w Active Directory

- Omówienie różnych typów grup zabezpieczeń w AD: uniwersalne, globalne, lokalne.
- Przykłady, jakie typy grup są odpowiednie w różnych scenariuszach związanych z dostępem do zasobów.

Grupa 5: Proces logowania w Active Directory

- Szczegółowe wyjaśnienie, jak przebiega proces uwierzytelniania i autoryzacji w Active Directory.
- Omówienie kroków od momentu, gdy użytkownik wpisuje dane logowania, aż do uzyskania dostępu.

Po zakończeniu ćwiczeń, każda grupa może przedstawić swoje prezentacje lub raporty reszcie uczestników. To pozwoli na wymianę wiedzy i zrozumienie różnych aspektów infrastruktury Active Directory oraz jak one współgrają.

Przykładowe rozwiązania zadań dla poszczególnych grup:

Grupa 1: Hierarchiczna struktura Active Directory

Zadanie: Omówienie hierarchicznej struktury jednostek organizacyjnych (OU) w Active Directory oraz przedstawienie korzyści wynikających z właściwego ułożenia OU w kontekście zarządzania.

Rozwiązanie:

- Hierarchiczna struktura OU w Active Directory jest wykorzystywana do organizowania obiektów (np. użytkowników, komputerów) w logiczne grupy, co ułatwia zarządzanie nimi.
- Przykłady korzyści: łatwiejsze zarządzanie uprawnieniami, spójne zastosowanie zasad grupowych, możliwość delegetowania uprawnień do zarządzania danymi grupami.

Grupa 2: Delegowanie kontroli w Active Directory

Zadanie: Wyjaśnienie procesu delegowania uprawnień w ramach Active Directory oraz podanie przykładów scenariuszy, w których delegowanie uprawnień jest ważne.

Rozwiązanie:

- Delegowanie uprawnień pozwala określonym użytkownikom lub grupom wykonywać określone zadania administracyjne bez potrzeby posiadania pełnych praw.
- Przykłady scenariuszy: delegowanie zarządzania danymi OU do lokalnych administratorów, umożliwienie helpdeskowi resetowania haseł użytkowników.

Grupa 3: Rola DNS w Active Directory

Zadanie: Wyjaśnienie, jak DNS (Domain Name System) odgrywa kluczową rolę w infrastrukturze Active Directory oraz dlaczego poprawna konfiguracja DNS jest istotna dla działania AD.

Rozwiązanie:

- DNS przypisuje nazwy domenowe do adresów IP, co umożliwia identyfikację i odnajdywanie zasobów w sieci.
- W Active Directory, nazwy domenowe są kluczowe, ponieważ to one identyfikują obiekty i usługi w sieci.
- Nieprawidłowa konfiguracja DNS może prowadzić do problemów z logowaniem, replikacją AD i ogólną niedostępnością zasobów.

Grupa 4: Grupy zabezpieczeń w Active Directory

Zadanie: Omówienie różnych typów grup zabezpieczeń w AD (uniwersalne, globalne, lokalne) oraz podanie przykładów, kiedy każdy typ grupy jest stosowany.

Rozwiązanie:

- Grupy globalne służą do zarządzania dostępem do zasobów w obrębie domeny.
- Grupy uniwersalne umożliwiają przypisywanie uprawnień do zasobów w różnych domenach.
- Grupy lokalne działają w kontekście pojedynczego komputera.
- Przykład: grupa globalna "Dostęp do drukarek" pozwala użytkownikom z różnych lokalizacji drukować na wspólnych drukarkach.

Grupa 5: Proces logowania w Active Directory

Zadanie: Szczegółowe wyjaśnienie procesu uwierzytelniania i autoryzacji w Active Directory, wraz z omówieniem kroków od momentu, gdy użytkownik wpisuje dane logowania, aż do uzyskania dostępu.

Rozwiązanie:

- Uwierzytelnianie to proces potwierdzenia tożsamości użytkownika na podstawie dostarczonych danych logowania.
- Autoryzacja następuje po uwierzytelnieniu i określa, jakie zasoby użytkownik ma prawo używać.
- Kolejne kroki obejmują: wpisanie danych logowania, przesłanie ich do kontrolera domeny, weryfikację w bazie danych, zwrócenie tokena uwierzytelniającego, który pozwala na dostęp do zasobów.

To są tylko przykładowe rozwiązania. Grupy mogą dodać więcej szczegółów, przykładów i prezentować je w formie prezentacji, raportu lub dyskusji.\