49 Podstawowe pojęcia związane z Active Directory

ZAGADNIENIA

- **Funkcja usługi Active Directory w systemie Windows Server**
- **Zastosowanie DNS**

Systemy operacyjne z rodziny Windows Server są przeznaczone do instalowania na komputerach odgrywających rolę serwerów w sieci. W systemach Windows Server można podzielić użytkowników i grupy na:

- **użytkowników lokalnych i grupy lokalne** – konta są tworzone na lokalnym komputerze i umożliwiają korzystanie z jego zasobów. Przechowywane są tylko na komputerach, na których zostały stworzone. Miejscem przechowywania kont jest baza **SAM** (ang. *Security Accounts Manager*) zapisana lokalnie na komputerze. Konta użytkowników lokalnych są inne na każdym komputerze, nawet gdy nazwy użytkowników są takie same.
- **użytkowników domenowych i grupy domenowe** – konta mają na celu logowanie się użytkowników do domeny, co umożliwia korzystanie z zasobów z dowolnego komputera przyłączonego do domeny. Konta użytkowników domenowych są przechowywane w **usługach katalogowych** (ang. *Active Directory*) na **kontrolerach domeny** i następnie replikowane między wszystkimi kontrolerami w domenie.

Active Directory (AD) jest to usługa katalogowa dla systemów Windows. Od systemu Windows 2008 otrzymała nazwę **Active Directory Domain Services** (AD DS), aby identyfikować usługę katalogową jako zapewniającą uwierzytelnianie zasobów w obrębie organizacji, w której usługi sieciowe kontroluje wewnętrzna domena, i zarządzanie nimi. Opisuje ona strukturę sieci i jej składników. Może pracować w trybie **natywnym** (ang. *native*) lub w **trybie zgodności** ze starszymi wersjami Windows. W trybie natywnym w sieci są obsługiwane tylko systemy Windows 2000 i nowsze. Jeżeli w sieci znajdują się komputery z systemami Windows Millenium i starszymi, to konieczny jest tryb zgodności, aby mogły one łączyć się do domeny. Domyślnie jest wybierany tryb natywny, a włączenie trybu zgodności jest możliwe w konfiguracji niestandardowej.

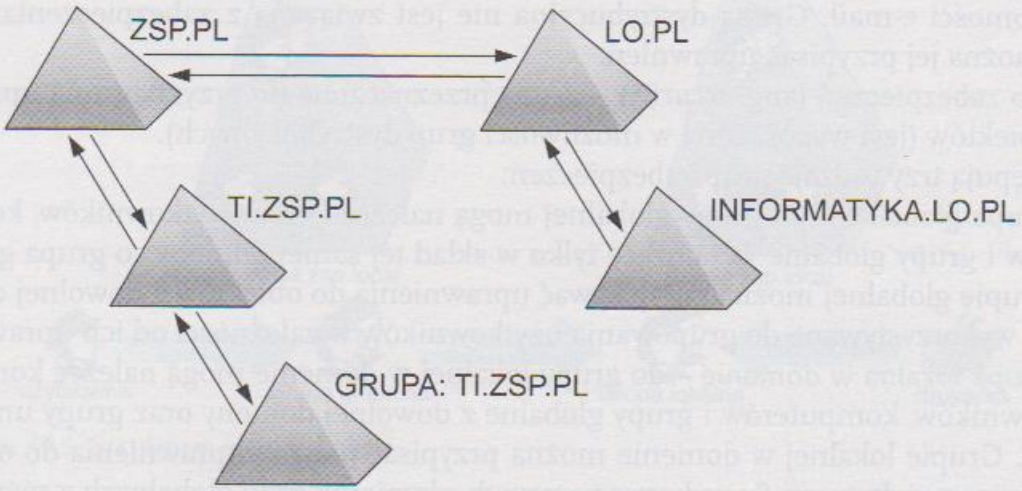
Active Directory jest przestrzenią nazw. **Przestrzeń nazw** (ang. *namespace*) to ograniczony obszar, w którego obrębie nazwa może być odnaleziona i wykorzystana do uzyskania dostępu do obiektu oraz jego atrybutów lub usług. Przykładem przestrzeni nazw może być system plików w systemie operacyjnym, w którym na podstawie nazwy plików i ścieżki dostępu możemy zlokalizować plik. Przestrzeń nazw w AD może być ciągła lub nieciągła. Przestrzeń jest **ciągła**, jeśli w całej strukturze istnieją dokładnie jeden obiekt typu **korzeń** (ang. *root*) i nazwa **obiektu podrzędnego** (ang. *child*) – powstaje przez dodanie prefiksu do nazwy obiektu **nadrzędnego** (ang. *parent*). Gdy nie ma jednego korzenia, przestrzeń jest **nieciągła**.

Obiekt to wyróżniony, nazwany zbiór atrybutów reprezentujący np. użytkownika, drukarkę lub komputer. Zbiór wszystkich możliwych rodzajów obiektów występujących w Active Directory i związanych z nimi atrybutów stanowi **schemat** (ang. *schema*).

W Active Directory podstawowym elementem konstrukcji jest **domena** (ang. *domain*). Domena to grupa komputerów połączonych w sieć, składająca się z serwera odgrywającego rolę kontrolera domeny oraz stacji roboczych – klientów współdzielących bazę katalogową. **Kontroler domeny** (ang. *domain controller*) przechowuje informacje o użytkownikach sieci i ich uprawnieniach. Dzięki temu informacje te są gromadzone w jednym miejscu i dostępne dla wszystkich klientów, co ułatwia zarządzanie siecią. W dużych sieciach może być więcej kontrolerów domeny, ale w takim przypadku wymieniają się między sobą przechowywanymi informacjami o sieci. Kontrolery domeny są równoprawne – każdy ma zapisywalną replikę tej samej bazy danych.

Domena wchodzi w skład **drzewa** (ang. *tree*), czyli związku wielu domen mających ten sam schemat, konfigurację i tworzących ciągłą hierarchiczną przestrzeń nazw. Przyłączenie domeny do drzewa jest określone w momencie instalacji jej pierwszego kontrolera.

Las (ang. *forest*) to struktura złożona z wielu drzew, także o wspólnym schemacie i konfiguracji, ale niemająca ciągłej przestrzeni nazw. Las może składać się z jednego drzewa lub wielu drzew. Przynależność do lasu jest określana w momencie instalacji pierwszego kontrolera domeny – przed określeniem przynależności do drzewa. Przykładowy las pokazano na rys. 49.1.



Rys. 49.1. Schemat lasu AD

Przestrzeń nazw w Active Directory została zorganizowana hierarchicznie. Obiekty typu **kontenery** mogą przechowywać inne obiekty. Nazwa obiektu w Active Directory opisuje jego położenie w strukturze hierarchicznej. Taką nazwę określa się mianem **pełnej nazwy DN** (ang. *Distinguished Name*).

Podstawowe składniki DN to:

- **DC** – komponent domenowy (ang. *domain component*),
- **CN** – nazwa (ang. *common name*),
- **OU** – jednostka organizacyjna (ang. *organizational unit*),
- **O** – organizacja (ang. *organization*).

Przykładowo: zapis **O=Internet/DC=PL/OU=ZSP/CN=uczen** oznacza, że obiekt *uczen* jest zlokalizowany w jednostce organizacyjnej ZSP domeny PL w organizacji **internet**.

Nazwa względna obiektu RDN (ang. *Relative Distinguished Name*) jest to część pełnej nazwy DN, zawierająca tylko atrybuty obiektu, np. w nazwie DN atrybutem obiektu jest **uczen** i jest to nazwa RDN tego obiektu.

Domena AD jest zorganizowana hierarchicznie, a jej podstawowym składnikiem jest **jednostka organizacyjna** (ang. *Organizational Unit*). Jest ona kontenerem, dzięki czemu może zawierać w sobie inne obiekty, co pozwala grupować zasoby i użytkowników oraz delegować prawa administracyjne. Jednostki organizacyjne mogą być uporządkowane hierarchicznie, np. w modelu geograficznym jednostki są tworzone zgodnie z lokalizacjami oddziałów firmy, natomiast w modelu organizacyjnym struktura jednostek powinna odpowiadać strukturze organizacyjnej firmy.

Oprócz jednostek organizacyjnych w Active Directory możemy tworzyć obiekty reprezentujące:

- użytkowników,
- komputery,
- drukarki,
- grupy,
- udostępnione foldery,
- kontakty.

Obiekty tworzone w Active Directory są reprezentantami rzeczywistych zasobów sieci. W Active Directory są dwie kategorie grup:

- **Grupa dystrybucyjna** (ang. *distribution*) – grupa używana jedynie do dystrybuowania wiadomości e-mail. Grupa dystrybucyjna nie jest związana z zabezpieczeniami, tzn. nie można jej przypisać uprawnień.
- **Grupa zabezpieczeń** (ang. *security*) – grupa przeznaczona do przyznawania uprawnień do obiektów (jest wyposażona w możliwości grup dystrybucyjnych).

  Występują trzy rodzaje grup zabezpieczeń:
  - **Grupa globalna** – do grupy globalnej mogą należeć konta użytkowników, komputerów i grupy globalne wchodzące tylko w skład tej samej domeny co grupa globalna. Grupie globalnej można przypisywać uprawnienia do obiektów z dowolnej domeny. Są wykorzystywane do grupowania użytkowników w zależności od ich uprawnień.
  - **Grupa lokalna w domenie** – do grupy lokalnej w domenie mogą należeć konta użytkowników, komputerów i grupy globalne z dowolnej domeny oraz grupy uniwersalne. Grupie lokalnej w domenie można przypisać jedynie uprawnienia do obiektów z tej samej domeny. Są wykorzystywane do skupiania grup globalnych z różnych domen, którym zostaną przydzielone takie same uprawnienia do obiektu (np. drukarki) znajdującego się w tej samej domenie co grupa lokalna.
  - **Grupa uniwersalna** – występuje jedynie w trybie natywnym. Mogą do niej należeć konta użytkowników, komputerów oraz grupy uniwersalne i globalne z dowolnej domeny. Grupie uniwersalnej można przypisać uprawnienia do obiektów z różnych domen.

Tworząc strukturę grup, należy przydzielić użytkowników do grup globalnych, przydzielić grupy globalne do grup lokalnych, a następnie nadać prawa grupom lokalnym.

PRZYKŁAD 49.1

Projektowanie struktury domen i grup w szkole

Szkolna sieć jest zbudowana z trzech domen. Domena główna o nazwie **`zsp.local`** ma dwie poddomeny: **`administracja.zsp.local`** oraz **`szkola.zsp.local`**. W domenie **`zsp.local`** znajduje się drukarka, z której mają korzystać użytkownicy z wszystkich domen.

- Należy utworzyć grupy, które umożliwią spełnienie powyższych wymagań. W każdej z domen trzeba zgrupować użytkowników mających prawo do drukowania i przypisać ich do grupy globalnej.

Domena AD jest zorganizowana hierarchicznie, a jej podstawowym składnikiem jest **jednostka organizacyjna** (ang. *Organizational Unit*). Jest ona kontenerem, dzięki czemu może zawierać w sobie inne obiekty, co pozwala grupować zasoby i użytkowników oraz delegować prawa administracyjne. Jednostki organizacyjne mogą być uporządkowane hierarchicznie, np. w modelu geograficznym jednostki są tworzone zgodnie z lokalizacjami oddziałów firmy, natomiast w modelu organizacyjnym struktura jednostek powinna odpowiadać strukturze organizacyjnej firmy.

Oprócz jednostek organizacyjnych w Active Directory możemy tworzyć obiekty reprezentujące:

- użytkowników,
- komputery,
- drukarki,
- grupy,
- udostępnione foldery,
- kontakty.

Obiekty tworzone w Active Directory są reprezentantami rzeczywistych zasobów sieci. W Active Directory są dwie kategorie grup:

- **Grupa dystrybucyjna** (ang. *distribution*) – grupa używana jedynie do dystrybuowania wiadomości e-mail. Grupa dystrybucyjna nie jest związana z zabezpieczeniami, tzn. nie można jej przypisać uprawnień.
- **Grupa zabezpieczeń** (ang. *security*) – grupa przeznaczona do przyznawania uprawnień do obiektów (jest wyposażona w możliwości grup dystrybucyjnych).

  Występują trzy rodzaje grup zabezpieczeń:
  - **Grupa globalna** – do grupy globalnej mogą należeć konta użytkowników, komputerów i grupy globalne wchodzące tylko w skład tej samej domeny co grupa globalna. Grupie globalnej można przypisywać uprawnienia do obiektów z dowolnej domeny. Są wykorzystywane do grupowania użytkowników w zależności od ich uprawnień.
  - **Grupa lokalna w domenie** – do grupy lokalnej w domenie mogą należeć konta użytkowników, komputerów i grupy globalne z dowolnej domeny oraz grupy uniwersalne. Grupie lokalnej w domenie można przypisać jedynie uprawnienia do obiektów z tej samej domeny. Są wykorzystywane do skupiania grup globalnych z różnych domen, którym zostaną przydzielone takie same uprawnienia do obiektu (np. drukarki) znajdującego się w tej samej domenie co grupa lokalna.
  - **Grupa uniwersalna** – występuje jedynie w trybie natywnym. Mogą do niej należeć konta użytkowników, komputerów oraz grupy uniwersalne i globalne z dowolnej domeny. Grupie uniwersalnej można przypisać uprawnienia do obiektów z różnych domen.

Tworząc strukturę grup, należy przydzielić użytkowników do grup globalnych, przydzielić grupy globalne do grup lokalnych, a następnie nadać prawa grupom lokalnym.

PRZYKŁAD 49.1

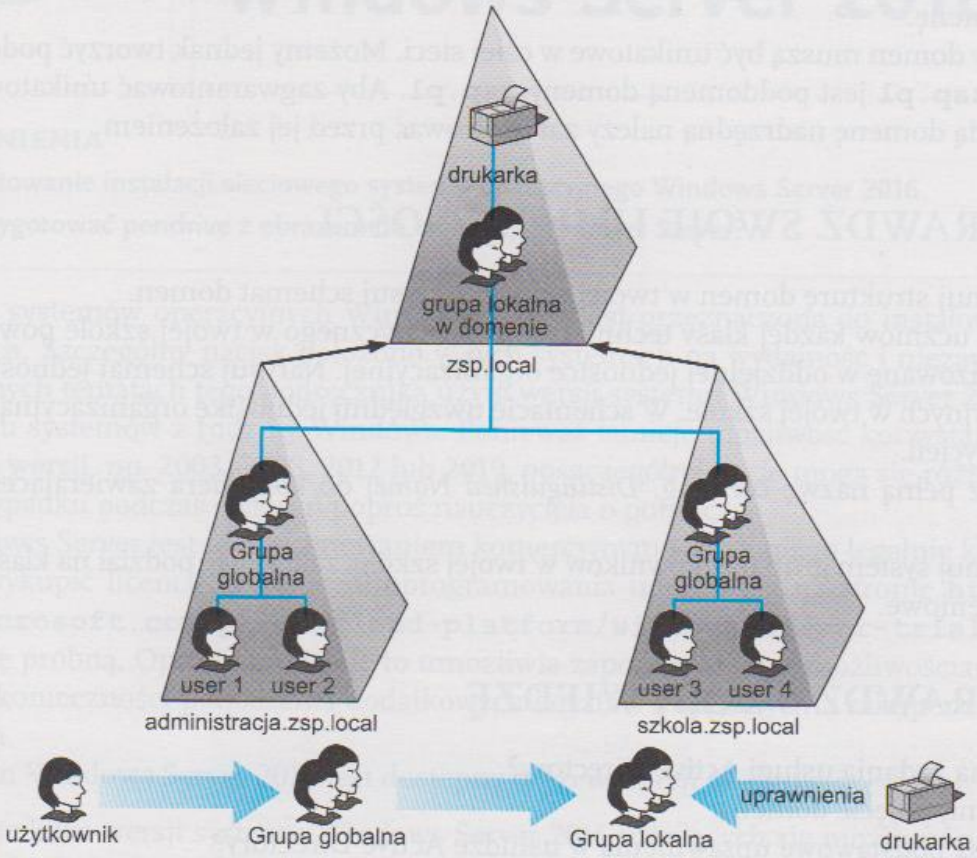
Projektowanie struktury domen i grup w szkole

Szkolna sieć jest zbudowana z trzech domen. Domena główna o nazwie **`zsp.local`** ma dwie poddomeny: **`administracja.zsp.local`** oraz **`szkola.zsp.local`**. W domenie **`zsp.local`** znajduje się drukarka, z której mają korzystać użytkownicy z wszystkich domen.

- Należy utworzyć grupy, które umożliwią spełnienie powyższych wymagań. W każdej z domen trzeba zgrupować użytkowników mających prawo do drukowania i przypisać ich do grupy globalnej.

- Grupy globalne z domen **administracja.zsp.local** i **szkola.zsp.local** należy przypisać do grupy lokalnej w domenie **zsp.local**.
- Trzeba też przypisać odpowiednie uprawnienia do drukarki grupie lokalnej w domenie.

Na rys. 49.2 pokazano strukturę sieci szkolnej, w której zrealizowano wymagania.



Rys. 49.2. Struktura sieci szkolnej

Active Directory zapewnia kontrolę dostępu do zasobów oraz informacji o obiektach przechowywanych w strukturze katalogowej przez weryfikację uprawnień. Administrator lub właściciel obiektu musi nadać prawa dostępu do niego, zanim ktokolwiek będzie korzystać z obiektu. Lista uprawnień jest przechowywana w AD i zawiera informację o tym, kto może wykonać operację i jaki jej rodzaj. Uprawnienia możemy **nadawać** (ang. *allow*) lub ich **zabronić** (ang. *deny*), przy czym zabranianie zawsze ma priorytet w stosunku do zezwolenia.

Jest pięć podstawowych uprawnień:

- **pełna kontrola** (ang. *full control*) – zmiana uprawnień, przejmowanie na własność oraz wszelkie pozostałe działania;
- **odczyt** (ang. *read*) – prawo odczytania listy uprawnień oraz wszystkich atrybutów wszystkich obiektów;
- **zapis** (ang. *write*) – prawo zmiany wszystkich atrybutów obiektów;
- **tworzenie wszystkich obiektów podrzędnych** (ang. *create all child objects*) – prawo tworzenia obiektów dowolnego typu wewnątrz OU;
- **usuwanie wszystkich obiektów podrzędnych** (ang. *delete all child objects*) – prawo usuwania obiektów dowolnego typu z OU.

Głównym mechanizmem wykorzystywanym przez Active Directory do identyfikacji obiektów jest system **DNS** (ang. *Domain Name System*). DNS służy do kojarzenia nazw i adresów IP. Domeny DNS są budowane w sposób hierarchiczny. Na różnych poziomach hierarchii występują domeny główne, podrzędne, a także komputery, np. **www.zsp.pl**, gdzie www jest nazwą komputera, a zsp – nazwą domeny szkoły w domenie pl. Nie można zainstalować Active Directory bez uprzednio zainstalowanego serwera DNS obsługującego tę domenę.

Nazwy domen muszą być unikatowe w całej sieci. Możemy jednak tworzyć poddomeny, np. **ti.zsp.pl** jest poddomeną domeny **zsp.pl**. Aby zagwarantować unikatowość nazwy, każdą domenę nadrzędną należy zarejestrować przed jej założeniem.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zaplanuj strukturę domen w twojej szkole. Narysuj schemat domen.
2. Konta uczniów każdej klasy technikum informatycznego w twojej szkole powinny być zlokalizowane w oddzielnej jednostce organizacyjnej. Narysuj schemat jednostek organizacyjnych w twojej szkole. W schemacie uwzględnij jednostkę organizacyjną dla kont nauczycieli.
3. Zapisz pełną nazwę **DN** (ang. *Distinguished Name*) do kontenera zawierającego twoje konto.
4. Zaplanuj system grup użytkowników w twojej szkole, zakładając podział na klasy i grupy ćwiczeniowe.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jakie są zadania usługi Active Directory?
2. Wyjaśnij pojęcie domeny.
3. Jakie są podstawowe uprawnienia w usłudze Active Directory?
4. Wyjaśnij, jaką funkcję pełni system DNS.