Co to jest Active Directory (Przypomnienie i uzupełnienie) ?

Usługa Active Directory przechowuje informacje o obiektach znajdujących się w sieci oraz umożliwia administratorom i użytkownikom łatwe znajdowanie tych informacji i korzystanie z nich. Usługa Active Directory używa magazynu danych o określonej strukturze jako podstawy dla logicznej i hierarchicznej organizacji informacji katalogowych. Ten magazyn danych, nazywany również katalogiem, zawiera informacje o obiektach usługi Active Directory. Do tych obiektów zazwyczaj należą zasoby udostępnione, takie jak serwery, woluminy, drukarki oraz konta użytkowników i komputerów w sieci. Usługą Active Directory są zintegrowane zabezpieczenia polegające na uwierzytelnianiu logowania i kontroli dostępu do obiektów w katalogu. Po jednokrotnym zalogowaniu sie do sieci administratorzy mogą zarządzać danymi katalogowymi i ich organizacja w sieci, a autoryzowani użytkownicy sieci maja dostęp do zasobów znajdujących się w dowolnym miejscu sieci. Administracja oparta na zasadach ułatwia zarządzanie nawet najbardziej złożoną siecią.

Ponadto usługa Active Directory obejmuje następujące elementy:

- Zestaw reguł, nazywany schematem, który określa klasy obiektów i atrybuty zawarte w katalogu, ograniczenia i limity dotyczące wystąpień tych obiektów oraz format ich nazw.
- Wykaz globalny, który zawiera informacje o każdym obiekcie w katalogu. Umożliwia on użytkownikom i administratorom znajdowanie informacji katalogowych, niezależnie od tego, która domena w katalogu zawiera te informacje.
- Mechanizm przeszukiwania i indeksowania, który umożliwia użytkownikom i aplikacjom w sieci publikowanie i znajdowanie obiektów i ich właściwości. Funkcja usługi Active Directory jest dostarczanie informacji o obiektach katalogu kwerendom przesyłanym przez użytkowników i programy. Administratorzy i użytkownicy mogą łatwo wyszukiwać informacje, używając polecenia Wyszukaj w menu Start. Programy klienckie mogą uzyskiwać dostęp do informacji w usłudze Active Directory, korzystając z interfejsów usługi Active Directory (ADSI).
- Usługa replikacji, która dystrybuuje dane katalogowe w sieci. Wszystkie kontrolery domeny w domenie uczestniczą w replikacji i zawierają pełna kopie wszystkich informacji katalogowych dla danej domeny. Każda zmiana danych katalogowych jest replikowana na wszystkich kontrolerach domeny w domenie.
- Obsługa oprogramowania klienta usługi Active Directory, dzięki której wiele funkcji systemu Microsoft Windows 2000 Professional lub Windows XP Professional jest dostępnych na komputerach z systemem Windows 95, Windows 98 lub Windows NT Server 4.0. Dla komputerów bez oprogramowania klienta usługi Active Directory katalog pojawia sie jako katalog systemu Windows NT.

Magazyn danych katalogowych

Usługa katalogowa Active Directory używa magazynu danych do przechowywania wszystkich informacji katalogowych. Ten magazyn danych często jest nazywany katalogiem. Katalog zawiera informacje o obiektach, takich jak użytkownicy, grupy, komputery, domeny, jednostki organizacyjne i zasady zabezpieczeń. Informacje te mogą być publikowane dla użytkowników i administratorów.

Katalog jest przechowywany na kontrolerach domeny i mogą do niego uzyskiwać dostęp aplikacje sieciowe lub usługi. Domena może zawierać jeden lub większa liczbę kontrolerów domeny. Każdy kontroler domeny przechowuje kopie katalogu dla całej domeny, w której sie znajduje. Zmiany wprowadzone w katalogu na jednym kontrolerze domeny są replikowane na innych kontrolerach domeny w domenie, drzewie domen lub lesie. Usługa Active Directory używa czterech róznych typów partycji katalogu do przechowywania i kopiowania róznych typów danych. Partycje katalogu zawierają dane dotyczące domeny, konfiguracji, schematu i aplikacji. Ten model magazynowania i replikacji zapewnia dostęp do informacji katalogowych użytkownikom i administratorom w całej domenie. Dane katalogowe są przechowywane w pliku Ntds.dit na kontrolerze domeny. Dane prywatne są bezpiecznie przechowywane, a publiczne dane katalogowe sa przechowywane w udostępnionym woluminie systemowym, skąd mogą być replikowane na innych kontrolerach domeny w domenie.

Schemat

Schemat usługi Active Directory zawiera definicje wszystkich obiektów znajdujących sie w katalogu. Kazdy nowo utworzony obiekt katalogu przed zapisaniem go w katalogu jest porównywany z odpowiednia definicja obiektu w celu sprawdzenia jego poprawności. Schemat składa sie z klas obiektów i atrybutów. Schemat podstawowy (domyślny) zawiera bogaty zestaw klas obiektów i atrybutów, który spełnia wymagania większości organizacji i jest zgodny ze standardem X.500 Międzynarodowej Organizacji Normalizacyjnej (ISO) dotyczącym usług katalogowych. Schemat jest rozszerzalny, wiec klasy i atrybuty schematu podstawowego można modyfikować, a także dodawać je do niego. Jednak każda ewentualna zmianę należy dokładnie przemyśleć, ponieważ rozszerzenie schematu wpływa na cała siec.
W schemacie klasa obiektów reprezentuje kategorie obiektów katalogu, na przykład użytkowników, drukarki czy aplikacje, które maja wspólny zestaw właściwości. Definicja każdej klasy obiektów zawiera listę atrybutów schematu, których można używać do opisania wystąpień klasy. Na przykład klasa **User** ma takie atrybuty, jak **givenName**, **surname** i **streetAddress**. Po utworzeniu nowego użytkownika w katalogu użytkownik ten staje sie wystapieniem klasy **User**, a wprowadzane informacje o tym użytkowniku staja sie wystapieniami atrybutów.

Schemat posiada następujące składniki:

Klasy obiektu
: Definiują obiekty, które mogą pojawić sie w katalogu oraz ich atrybuty.

Dziedziczenie klas
: Definiuje metodę tworzenia nowych klas obiektów na podstawie istniejących klas.

Atrybuty obiektu
: Definiują dostępne atrybuty. Określają również działania, które mogą być wykonywane na klasach obiektu.

Zasady strukturalne
: Określają możliwość zarządzania drzewem katalogu. Definiuje w jakich kontenerach mogą znaleźć sie określone obiekty.

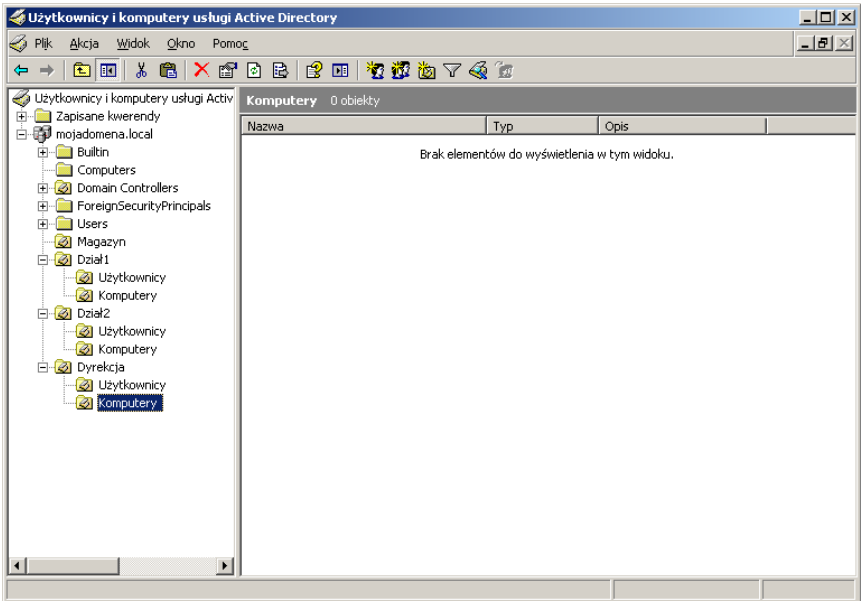
Zasady składni
: Określają typ wartości atrybutu, która może być przechowywana w katalogu.

Zasady zawartości

Określają atrybuty, które mogą być związane z dana klasa.

Jednostki Organizacyjne

Szczególnie przydatnym typem obiektu katalogu zawartym w domenie jest jednostka organizacyjna. Jednostki organizacyjne sa kontenerami usługi Active Directory, w których można umieszczać użytkowników, grupy, komputery i inne jednostki organizacyjne. Jednostka organizacyjna nie może zawierać obiektów z innych domen. Jednostka organizacyjna jest najmniejszym zakresem lub jednostka, której można przypisać ustawienia zasad grupy lub udzielić pełnomocnictw administracyjnych. Korzystając z jednostek organizacyjnych, można tworzyć kontenery z domena reprezentująca hierarchiczna, logiczna strukturę firmy. Pozwala to na zarządzanie konfiguracja oraz na korzystanie z kont i zasobów na podstawie modelu organizacyjnego. Na przykład: Rys. 1



Rys. 1. Przykład zastosowania jednostek organizacyjnych

Klienty Active Directory

Z możliwości Active Directory korzysta wiele usług i programów w systemie Windows. Najważniejsze z nich to:

- Zdalne uwierzytelniane i rozpoznawanie umiejscowienia w sieci. Użytkownik może załogować sie do kontrolera domeny, który znajduje sie najbliżej danego klienta w sieci. Dostępne jest także uwierzytelnianie.
- Interfejsy usługi Active Directory (ADSI) zapewniają wspólny interfejs API programistom tworzącym aplikacje dla usługi Active Directory. Pozwala także na pisanie skryptów korzystających z usług katalogowych.
- Rozproszony system plików (DFS). Możliwy jest dostęp do zasobów udostępnionych systemu DFS znajdujących sie na maszynach Windows Server 2003.
- Książka adresowa oraz programy pocztowe. Udostępnia informacje, takie jak numery telefonów i adresy. Pozwala także modyfikować te informacje.

- Możliwości wyszukiwania. Za pomocą menu wyświetlanego po kliknięciu przycisku Start można odszukać drukarki i osoby.

Konfiguracja Active Directory

Do konfiguracji usługi Active Directory służą trzy przystawki MMC:

1. Użytkownicy i komputery usługi Active Directory
2. Domeny i relacje zaufania usługi Active Directory
3. Lokacje i usługi Active Directory

Do zarządzania zawartością katalogu służy narzędzie: *Użytkownicy i komputery usługi Active Directory*. Po uruchomieniu przystawki i rozwinięciu węzła domeny w widoku drzewa konsoli jest wyświetlanych kilka kontenerów. Zaraz po utworzeniu kontrolera domeny domyślnie są wyświetlane następujące kontenery:

Builtin (Wbudowane)
: Zawiera obiekty, które określają domyślne grupy wbudowane, takie jak Operatorzy kont czy Administratorzy.

Computers (Komputery)
: Zawiera obiekty typu komputer z systemem Windows 2000, Windows XP lub Windows Server 2003, w tym konta komputerów utworzone pierwotnie za pomocą interfejsów programowania aplikacji (API), które nie mogły używać usługi Active Directory. Obiekty typu komputer są przenoszone do kontenera Computer podczas uaktualniania domen systemu Windows NT do systemu operacyjnego serwera Windows 2000 lub Windows Server 2003.

Domain Controllers (Kontrolery domen)
: Zawiera obiekty typu komputer z systemem Windows 2000 lub Windows Server 2003, pełniące rolę kontrolerów domeny.

Users (Użytkownicy)
: Zawiera konta użytkowników i grup utworzone pierwotnie za pomocą interfejsów API, które nie mogły korzystać z usługi Active Directory. Konta użytkowników i grup są przenoszone do kontenera Użytkownicy podczas uaktualniania domen systemu Windows NT do systemu operacyjnego serwera Windows 2000 lub Windows Server 2003. Do modyfikowania kont użytkowników i grup utworzonych pierwotnie za pomocą interfejsów API, które nie mogły korzystać z usługi Active Directory, można używać narzędzia Menedżer użytkowników systemu Windows NT 4.0 (**Usrmgr**).

Po wybraniu polecenia Funkcje zaawansowane w menu Widok w konsoli są wyświetlane dwa dodatkowe foldery:

LostAndFound (Zgubione-Znalezione)
: Zawiera obiekty, których kontenery zostały usunięte w momencie tworzenia tych obiektów. Jeśli obiekt zostanie utworzony w lokalizacji, która nie istnieje po replikacji, lub zostanie przeniesiony do takiej lokalizacji, staje się obiektem „zgubionym” i zostaje umieszczony w kontenerze Zgubione-Znalezione. Kontener

LostAndFoundConfig w partycji katalogu konfiguracji służy do tego samego celu w przypadku obiektów na poziomie lasu.

System (System)

Zawiera wbudowane ustawienia systemowe dla kontenerów i obiektów różnych usług systemowych.

Wybierając polecenie Opcje filtru w menu Widok, można wyświetlić wszystkie obiekty lub tylko wybrane obiekty, określić liczbę elementów, które mają być wyświetlane dla każdego folderu, a także utworzyć filtry niestandardowe za pomocą atrybutów obiektów i kwerend LDAP.

Narzędzia administracyjne

Narzędzia konsolowe

Do konfiguracji usług katalogowych możemy użyć narzędzi konsolowych:

dsadd

Dodaje obiekty do katalogu.

dsget

Powoduje wyświetlenie właściwości obiektów w katalogu.

dsmod

Modyfikuje wybrane atrybuty istniejącego obiektu w katalogu.

dsquery

Znajduje obiekty w katalogu zgodne z określonymi kryteriami wyszukiwania.

dsmove

Przenosi obiekt z bieżącej lokalizacji do nowej lokalizacji nadrzędnej.

dsrm

Usuwa obiekt, pełne poddrzewo znajdujące się poniżej obiektu w katalogu lub oba te elementy.

Schemat usługi Active Directory

Pozwala na modyfikowanie schematu katalogu. Przystawka *Schemat usługi Active Directory* nie jest domyślnie zainstalowana. Aby ją zainstalować należy:

- Otwórz okno wiersza polecenia.
- Wpisz polecenie:

regsvr32 schmmgmt.dll

- Kliknij przycisk *Start*, kliknij polecenie *Uruchom*, wpisz polecenie *mmc* , a następnie kliknij przycisk OK.
- W menu *Plik* kliknij polecenie *Dodaj/Usuń przystawkę*, a następnie kliknij przycisk *Dodaj*.
- W obszarze *Dostępne przystawki autonomiczne* kliknij dwukrotnie pozycję *Schemat usługi Active Directory*, kliknij przycisk *Zamknij*, a następnie kliknij przycisk *OK*.

- Aby zapisać tę konsolę, w menu *Plik* kliknij polecenie *Zapisz*.
- W polu *Zapisz* wskaż folder *główny_katalog_systemowy**system32*.
- W polu *Nazwa pliku* wpisz *schmmgmt.msc*, a następnie kliknij przycisk *Zapisz*.

ntdsutil

Ntdsutil.exe to narzędzie wiersza polecenia, które zapewnia funkcje zarządzania przeznaczone dla usługi Active Directory. Narzędzia Ntdsutil.exe można używać do wykonywania zadań związanych z konserwacją bazy danych usługi Active Directory.

Zadania 1

1. Utwórz hierarchię jednostek organizacyjnych AD (np.: firma, dyrekcja, sprzedaż, produkcja, administracja, logistyka, marketing, komputery, użytkownicy);
2. Utwórz trzech nowych użytkowników AD;
3. Utwórz trzy nowe kontakty AD;
4. Spróbuj zmodyfikować schemat katalogu;
5. Sprawdź działanie narzędzi konsolowych wymienionych w instrukcji.

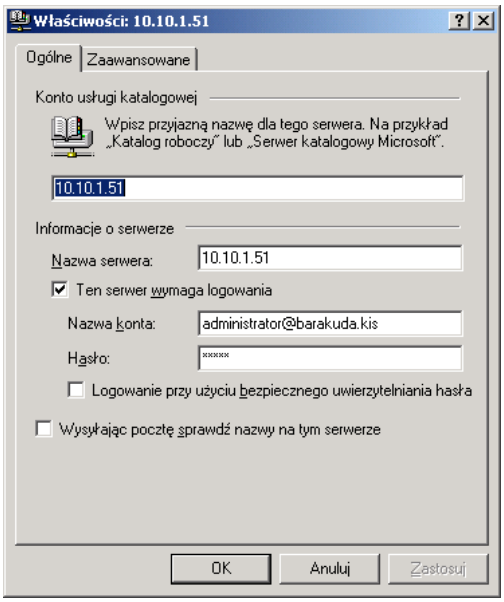
Wykorzystanie Active Directory - przykłady

Najistotniejsza funkcjonalność Active Directory wykorzystuje system Windows. Dzięki usłudze katalogowej możliwa jest zdalna autoryzacja użytkowników i komputerów, wyszukiwanie komputerów, użytkowników, drukarek itd. Umożliwia ona także wygodne zarządzanie zasobami plikowymi. Oprócz wewnętrznych usług systemowych katalog Active Directory może być wykorzystany przez aplikacje zewnętrzne. Możliwość ta zostanie pokazana na przykładzie dwóch aplikacji pocztowych, które z katalogu pobierać będą dane adresowe.

Wykorzystanie Active Directory w programie Outlook Express

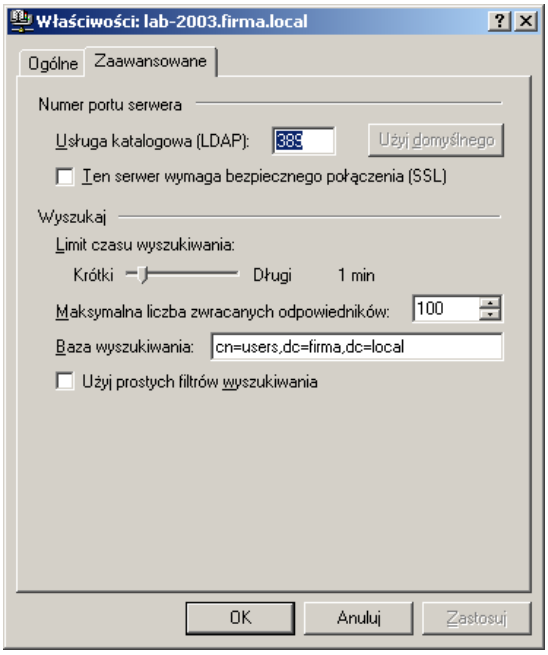
Jeśli używamy programu Outlook Express na komputerze pełniącym funkcję kontrolera domeny, dostęp do bazy adresowej powinien być skonfigurowany. Jeśli próbujemy pobrać dane z katalogu używając innego komputera (nawet nie należącego do domeny) należy przeprowadzić następująca procedurę:

- Wybrać ***Narzędzia->Konta***
- Następnie dodać w zakładce ***Usługi katalogowe*** nową książkę adresową poleceniem ***Dodaj->Usługa katalogowa***
- W kolejnych krokach kreatora należy podać nazwę serwera (lub jego adres IP)
- Po zakończeniu pracy kreatora wybrać ***Właściwości*** nowej usługi katalogowej
- W oknie dialogowym uzupełnić następujące pola (Rys. 2);:
    - *Nazwa serwera* - podać nazwę serwera lub jego adres IP, np.: *mojadomena.local*
    - zaznaczyć opcję: *Ten serwer wymaga logowania*
    - *Nazwa konta* - wpisać nazwę użytkownika, która będzie używana podczas logowania, np. *Administrator@mojadomena.local*
    - *Hasło* - podać hasło, które będzie używane podczas logowania, np. *P@$$word*



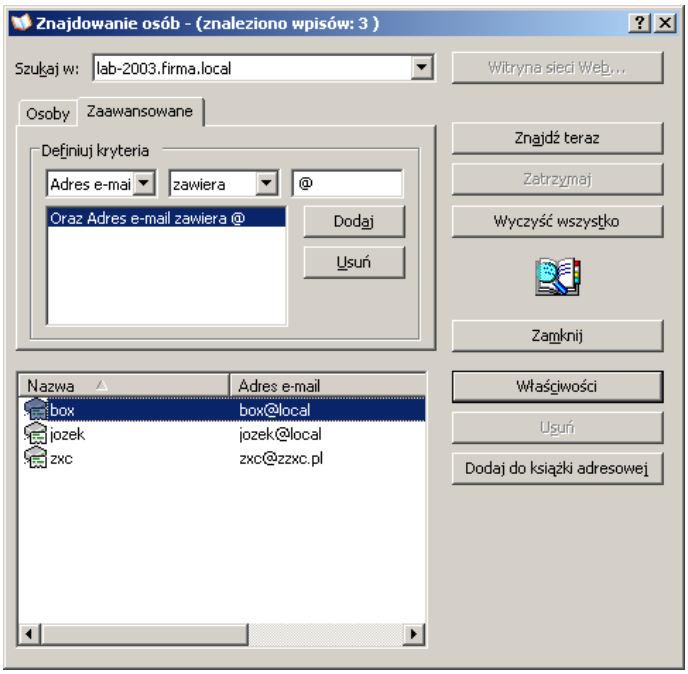
Rys. 2. W trakcie konfiguracji należy zaznaczyć opcję **Logowanie przy użyciu bezpiecznego uwierzytelniania hasła**

- Wybrać zakładkę *Zaawansowane* i wypełnić pola (Rys. 3):
  - *Baza wyszukiwania* - podać kontener, który będzie przeszukiwany, np.: *cn=users,dc=mojadomena,dc=local*;



Rys. 3. Konfiguracja książki adresowej LDAP w Outlook - zaawansowane

Aby skorzystać z udostępnionych danych należy otworzyć książkę adresową i wybrać funkcje *Edycja->Znajdź->Osoby*. Podczas wyszukiwania należy wybrać w *Szukaj w:* zdefiniowana wcześniej usługę katalogowa (Rys. 4).



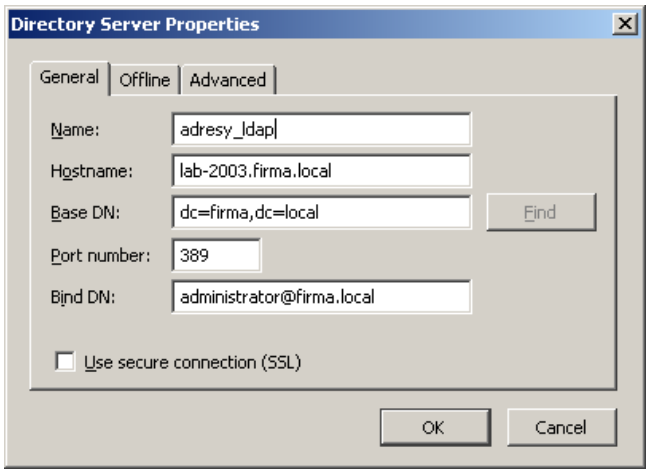
Rys. 4. Wyszukiwanie adresów w Outlook

Wykorzystanie Active Directory w programie Thunderbird

Aplikacja Mozilla Thunderbird nie jest zaprojektowana z myślą o Active Directory (podobnie jak większość klientów poczty nie pochodzących od Microsoftu). Nie występuje w niej zatem opcja przyłączenia do tej usługi. Należy więc w tym przypadku wykorzystać zgodność Active Directory z protokołem LDAP. Aby to zrobić należy:

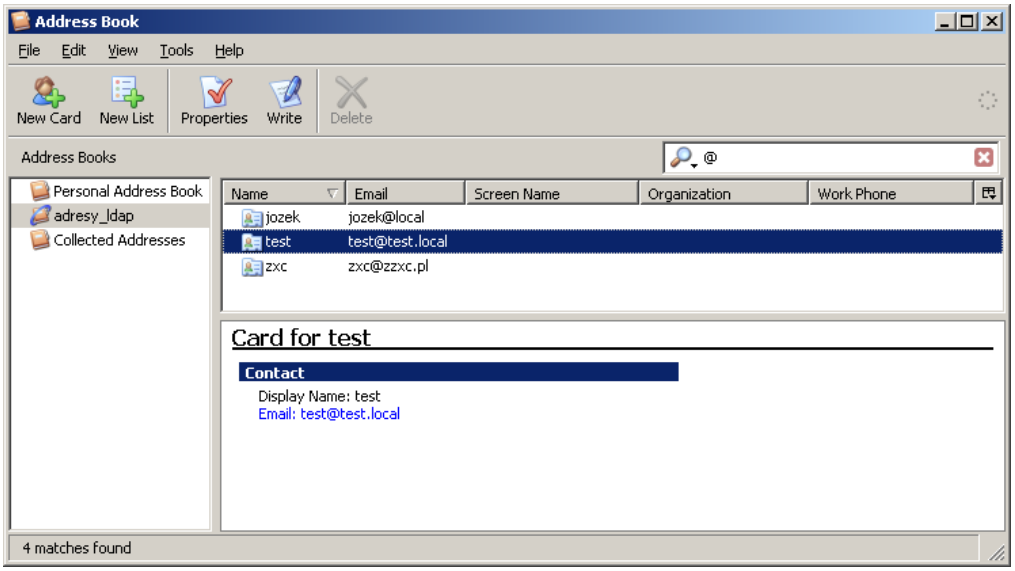
- Pobrać aplikację ze strony http://www.thunderbird.pl/.

- Uruchomić książkę adresową *Narzędzia->Książka adresowa*
- Następnie w książce adresowej wybrać *Plik->Nowy->katalog LDAP*
- Wypełnić okno dialogowe (Rys. 5):
    - Name - podać nazwę książki adresowej np.: 'Książka z katalogu'
    - Hostname - podać adres usługi katalogowej, np.: mojadomena.local
    - Base DN - podać nazwę przeszukiwanego kontenera, np.: cn=users,dc= mojadomena,dc=local
    - Port Number - 389
    - Bind DN - podać nazwę użytkownika, np,: Administrator@mojadomena.local



Rys. 5. Konfiguracja książki adresowej LDAP w Mozilla Thunderbird

Aby wyszukać dane katalogowe należy wpisać poszukiwany fragment nazwy lub adresu w pole wyszukiwania (w przykładzie została wpisana '@' aby wyświetlić wszystkich użytkowników ze zdefiniowanym adresem mailowym) (Rys. 6).



Rys.6. Wyszukiwanie adresów w Thunderbird

Zadania 2

- Skonfiguruj książkę adresowa w programie Outlook Express na kontrolerze domeny;
- Zainstaluj Mozillę Thunderbird i skonfiguruj książkę adresową LDAP;