

VII Seminarium PLOUG
Warszawa
Marzec 2003

Serwery LDAP w środowisku produktów Oracle

Mariusz Przybyszewski

maniekp@altkom.com.pl

maniekp@poczta.fm

<http://oraforum.altkom.com.pl>

Altkom Akademia

Wprowadzenie do LDAP

Często spotykamy się z problemem autentykacji użytkowników w środowiskach heterogenicznych i homogenicznych. Nigdy nie wiadomo, która z części naszej architektury ma przechowywać informacje o użytkownikach. Czy ma to być baza danych czy system operacyjny:

- Baza danych – informacje przechowywane jako użytkownicy bazy danych
- System operacyjny – informacje przechowywane jako użytkownicy systemu operacyjnego.

Często stosowanym sposobem na rozwiązanie tego problemu jest zastosowanie dedykowanego modułu, w którym przechowywane są informacje o użytkownikach i grupach. Takie moduły tworzone są zazwyczaj przez zastosowanie dodatkowych tabel w naszej aplikacji i zapisaniu w nich informacji o użytkownikach. Występuje tu jednak pewna wada – otóż sami musimy synchronizować hasła pomiędzy naszymi użytkownikami a użytkownikami baz danych i użytkownikami systemu operacyjnego. Wszystko *jest do zrobienia* pod jednym warunkiem, że hasła będą zmieniane wyłącznie przez naszą aplikację, jeśli jednak ktoś je zmieni poza nią - informacje nie będą spójne.

Baza danych ORACLE od dawna umożliwia uwierzytelnienie przez system operacyjny. Geneza tego rozwiązania tkwi w początkach, kiedy to użytkownicy łączyli się terminalami do systemu/hosta, na którym znajdowała się baza danych. Dlatego nie było potrzeby ponownego logowania się do bazy - po co uwierzytelniać ich jeszcze raz.

Ponieważ dziś klienci logują się do swoich systemów operacyjnych a baza do swojego, mechanizm ten nie jest już zabezpieczeniem. Często są to różne systemy, które nie współdziałają ze sobą.

Idealnym rozwiązaniem jest zastosowanie dedykowanego systemu przeznaczonego do przechowywania informacji o użytkownikach i udostępniającego te informacje zarówno dla systemu operacyjnego jak i bazy danych.

Dla takich celów został stworzony standard LDAP (Lightweight Directory Access Protocol). Słowo *lekki* wzięło się dlatego, że specyfikacja ta definiuje cienkiego klienta, który korzysta z katalogów wspierających model katalogu X.500 (oryginalnie X.500 wymaga grubych klientów).

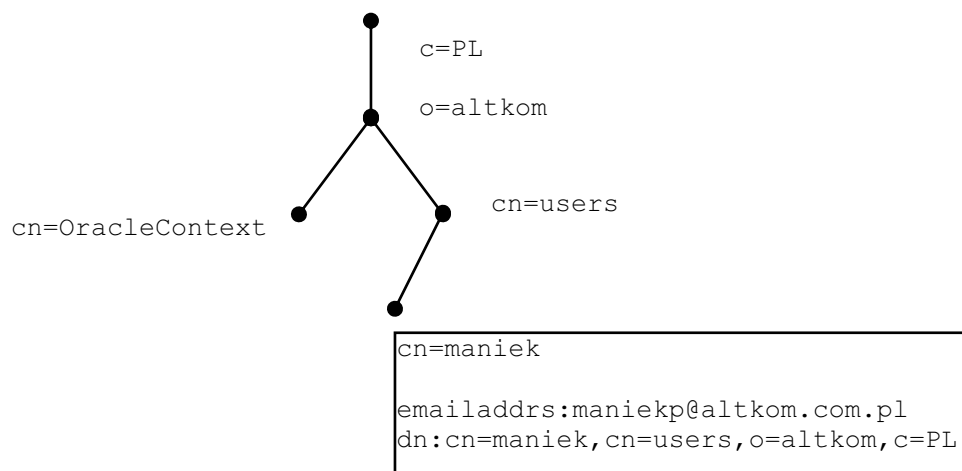
Aktualnie dostępna jest wersja LDAPv3. Standard LDAP został zatwierdzony przez IETF (Internet Engineering Task Force), a cała jego specyfikacja dostępna jest w postaci dokumentów RFC (Request For Comments).

Klient LDAP ma możliwość wykonania następujących funkcji:

- bind/unbind - zalogowanie się do serwera
- search – pobranie/wyszukanie informacji
- compare – sprawdzenie/porównanie zadanych wartości
- modify – wprowadzanie/usuwanie/modyfikacja

Informacje w katalogu są przechowywane w postaci wpisów (*Entries*). Każdy wpis jest obiektem jednej lub wielu klas. Klasy mogą być dziedziczone. Każda klasa składa się z jednego lub wielu atrybutów, które mogą być opcjonalne lub obowiązkowe. Istnieje wiele podstawowych typów atrybutów. Atrybuty mogą mieć więcej niż jedną wartość. Można tworzyć swoje klasy i atrybuty.

Wpisy są identyfikowane jednoznacznie przez **DN** (*Distinguished Name*). Mogą być również identyfikowane względem nadrzędnego wpisu (kontekstu) poprzez **RDN** (*Relational DN*).



Dostęp do wpisu chroniony jest poprzez listy kontroli dostępu (ACL – Access Control List). Można tworzyć uprawnienia dla kontekstów, wpisów oraz poszczególnych atrybutów.

Wpisy mogą być eksportowane/importowane do/z plików tekstowych w specjalnych formacie LDIF (LDAP Data Interchange Format).

Istnieje wiele implementacji serwerów LDAP. Wśród nich znajdują się takie, które są dedykowane wyłącznie dla LDAP jak i takie, które wspierają umożliwiając wiele dostępu do informacji, w tym LDAP.

Do najbardziej znanych należą:

- Sun ONE Directory Server
- Netscape Directory Server
- Novell eDirectory
- IBM Directory Server
- MS Active Directory
- Oracle Internet Directory
- OpenLDAP

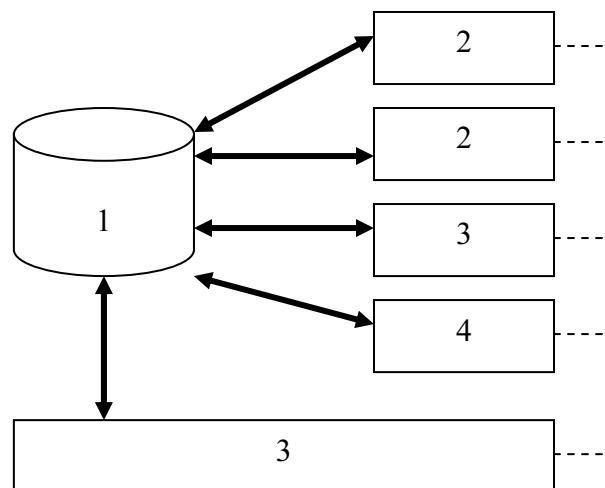
Oczywiście w serwerach LDAP nie są przechowywane informacje wyłącznie o użytkownikach – dla wielu systemów LDAP to repozytorium, które przechowuje typowe dla nich informacje. Przykładem może tu być przechowywanie adresów/nazw TNS – dzięki czemu każdy klient ORACLE nie musi posiadać pliku TNSNAMES.ORA.

Rodzaj przechowywanych informacji zależy już od twórców systemów. Należy jednak kierować się zasadą, że bazy katalogowe optymalizowane są do odczytu a nie do modyfikacji. Często przy operacjach masowych – lepiej usunąć i dodać na nowo.

Oracle Internet Directory

Oracle Internet Directory (OID) składa się z następujących składników:

1. Baza danych – repozytorium wpisów
2. Procesy serwera (oidldapd)– realizują żądania klientów
3. Procesy replikacji (oidrepd)– realizują replikację katalogów
4. Procesy integracji (odisrv)– realizują funkcje integracji OID z innymi serwerami LDAP i aplikacjami
5. Proces strażnika (oidmon)– inicjuje, kontroluje dostępność i kończy pozostałe procesów serwera.



Instalacja

Aby zainstalować OID należy uruchomić instalację serwera i wybrać odpowiednią opcję. Podczas instalacji istnieje możliwość wykorzystania istniejącej bazy lub utworzenie nowej. Zalecane jest wyodrębnienie osobnej bazy dla OID.

Po instalacji serwer jest dostępny pod domyślnym portem 389/636. Domyślnym administratorem jest „cn=orcladmin” z hasłem „welcome”, które należy zaraz po instalacji zmienić!

Instalacja OID nie jest wymagana w produkcie Internet Application Server 9iR2, gdzie serwer OID jest jednym z podstawowych składników Infrastructure i jest instalowany razem z oprogramowaniem serwera aplikacji. Hasło użytkownika „cn=orcladmin” jest ustawiane podczas instalacji – użytkownik podaje hasło administratora do wszystkich usług IAS.

Dane OID przechowywane są w bazie danych, w schemacie ODS, który ma również standardowe hasło „ODS”. Zaleca się jego zmianę przez program linii poleceń – *oidpasswd*.

Administracja

OID umożliwia „okienkową” administrację serwerem. Do tego celu służy narzędzie Oracle Directory Manager. Aby je uruchomić należy wybrać odpowiednią opcję w menu (Windows) lub uruchomić program *oidadmin* (Unix/Linux).

Ponieważ wszystkie informacje w OID są przechowywane jako wpisy, w tym także sama konfiguracja serwera, do zmiany ustawień można użyć standardowych programów linii poleceń. Należą do nich między innymi:

- *ldapadd[mt]* – dodaje nowy wpis [wielowątkowo – dla większej ilości]
- *ldapmodify[mt]* – modyfikuje istniejący wpis [wielowątkowo – dla większej ilości]
- *ldapdelete* – usuwa zadany wpis

Ponadto do standardowych operacji dedykowane są:

- *ldapbind* – test autentykacji do serwera
- *ldapmoddn* – zmienia DN istniejącego wpisu
- *ldapsearch* – wyszukuje informacje
- *ldapcompare* – porównuje wartość zadaną z wartością atrybutu w LDAP

Do ładowania/eksportu masowego dedykowane są:

- *bulkmodify* – pozwala na masowe modyfikacje wybranych atrybutów

- **bulkload** – używa SQLLoader do ładowania wpisów do OID
- **bulkdelete** – pozwala na usunięcie całego poddrzewa
- **ldifwrite** – tworzy plik LDIF zawierający dany kontekst

Uruchamianie i zamykanie możliwe jest poprzez serwis (Windows) lub programy linii poleceń: **oidmon** oraz **oidctl**. Istnieje możliwość definicji kilku konfiguracji serwera OID. Każda konfiguracja identyfikowana jest przez numer. Do składników konfiguracji należą:

- porty
- maksymalna ilość połączeń do bazy danych
- maksymalna ilość procesów serwera
- położenie portfela (atrybut wykorzystywany w połączeniach SSL)
- poziom autentykacji SSL (atrybut wykorzystywany w połączeniach SSL)

Aby uruchomić instancje serwera z odpowiednią konfiguracją należy przekazać jej numer programu **oidctl**. Zalecane jest utworzenie dodatkowej konfiguracji wykorzystywanej dla połączeń SSL. Zabezpiecza to nas przed ewentualnymi błędami, które nie mogą być poprawione gdy serwer nie jest uruchomiony.

Do zarządzania wpisami o użytkownikach i grupach dedykowany jest program DAS (Delegate Administration Service). Jest on dostępny w wersji WWW i działa w technologii Java Servlets.

Standardowo OID generuje logi operacji, które mogą przydać się podczas rozwiązywanie ewentualnych problemów. Pliki logów znajdują się w katalogu \$ORACLE_HOME/ldap/log (%ORACLE_HOME%\ldap\log - Windows). Poziom tych logów można ustalać.

Dodatkowo można monitorować operacje wykonywane podczas sesji OID. Wówczas dane te przechowywane są w serwerze OID. Do zmiany poziomu logowania i monitorowania należy użyć narzędzia Oracle Directory Manager lub narzędzi linii poleceń.

Możliwe jest definiowanie polis haseł dla użytkowników OID. W każdej polisie znajdują się między innymi restrykcje dotyczące:

- czasu wygasania hasła
- minimalnej długości hasła
- znaków wymaganych w hasle – duże/małe litery oraz cyfry.

Hasła używane podczas uwierzytelniania użytkowników są przechowywane w postaci zaszyfrowanej algorytmami jednostronnymi – nie można ich odszyfrować.

Uwierzytelnianie i autoryzacja

Istnieją następujące sposoby uwierzytelnień:

- anonimowe – klient ma prawa wbudowanego użytkownika *guest*
- na hasło – użytkownik loguje się poprzez dn/hasło
- SSL – następuje wymiana certyfikatów
- PROXY – wykorzystywane przez aplikacje, która uwierzytelnia się na hasło użytkownika PROXY, a następnie działa w imieniu danego użytkownika. Takie uwierzytelnienie stosuje serwis DAS.

Autoryzacja wykonywana jest podczas wykonywania jest podczas operacji, a nie po uwierzytelnieniu.

Partycje i repliki

Niekiedy uzasadnione jest utworzenie wielu fizycznie odrębnych katalogów, które odpowiadają wycinkom drzewa całej organizacji. Mamy wtedy do czynienia z partycjonowaniem katalogu.

Wówczas w drzewie głównym, znajdują się odnośniki na wpisach partycjonowanych, które zawierają informacje na temat adresu serwera danego wpisu. Z uwagi na wydajność nie jest zalecane tworzenie dużej ilości partycji.

Ponadto serwer OID może posiadać swoje repliki. Ma to nie kwestionowany wpływ na dostępność informacji przechowywanych w repozytorium. Do tworzenia repliki zalecane jest wykorzystanie „zimnej kopii” bazy oryginalnej.

Subskrybenci

Często zdarza się, że użytkownicy nie znajdują się w jednym kontekście. Wynika to ze struktury organizacyjnej firmy lub ze sposobu współdzielenia informacji z innymi korporacjami (wiele korporacji może korzystać z tego samego katalogu). Wówczas mamy do czynienia z subskrybentami. Innymi słowy subskrybenci to *konteksty*, które przechowują użytkowników i grupy. W każdym kontekście subskrybenta znajdują się wpisy:

- „cn=users” – przechowuje użytkowników
- „cn=groups” – przechowuje grupy
- „cn=OracleContext” – poddrzewo dedykowane produktom i usługom ORACLE. Istnieje również globalny „cn=OracleContext”, który zawiera m.in. informacje o domyślnym subskrybencie, oraz o położeniu pozostałych subskrybentów.

Platforma integracyjna

Platforma integracyjna (DIP – Directory Integration Platform) umożliwia:

- powiadamianie zainteresowanych aplikacji o zmianach w repozytorium (Provisioning)
- synchronizację wpisów z innymi katalogami (Synchronization)

Różnica pomiędzy w/w usługami polega na tym, że synchronizacja działa w dwie strony, natomiast powiadamianie tylko w jedną.

Obydwie metody opierają się na logach zmian, które są tworzone podczas modyfikacji wpisów w OID. Takie logi są następnie dystrybuowane do serwisu powiadamiania oraz/lub serwisu synchronizacji.

Wtyczki

Serwer OID umożliwia napisanie wtyczek, które są uruchamiane razem lub zamiast standardowych operacji. Wtyczki mogą być podłączane przez operację, po operacji lub zamiast operacji (tylko operacja *compare* i *modify*). Aktualnie istnieje możliwość implementacji wtyczki tylko w języku PL/SQL.

Interfejsy programistyczne

Interfejsy dostępne są dla języków:

- PL/SQL (pakiety DBMS_LDAP i DBMS_LDAP_UTL)
- C/C++ (biblioteki)
- JAVA (interfejs JNDI)

Powyższe interfejsy pozwalają na podłączanie się do OID jak i innych serwerów LDAP. Ponadto umożliwiają podpinanie się aplikacji na powiadomienia (Provisioning).

Wykorzystanie serwera OID w produktach ORACLE

Serwer Oracle Internet Directory jest lub może być wykorzystywany we wszystkich produktach ORACLE. Zaliczają się do nich m.in.:

- Oracle Database

- Oracle Portal
- Oracle Single Sign On
- Oracle Forms/Reports Services
- Oracle Containers for J2EE

Integracja z Oracle Database

Baza danych może wykorzystywać OID do autentykacji i autoryzacji użytkowników. Wykorzystywany jest tu mechanizm użytkowników korporacyjnych (*Enterprise Users*), który jest częścią opcji Advanced Security.

Aby używać tego mechanizmu, należy:

- zarejestrować bazę danych w serwerze OID
- utworzyć role korporacyjne w serwerze OID
- utworzyć role globalne w bazie danych
- utworzyć schematy globalne w bazie danych
- zmapować role korporacyjne na role globalne
- przypisać schematy globalnych do użytkowników OID

Do wykonywania powyższych czynności służy narzędzie Enterprise Security Manager. Rejestrowanie bazy może być również wykonane przez Database Configuration Assistant. Aby mechanizm zadziałał niezbędna jest też dwustronna konfiguracja SSL pomiędzy bazą danych a OID. Klient może podłączać się do bazy zarówno poprzez hasło jak i certyfikat SSL.

Ponadto OID służyć do przechowywania nazw TNS z definicjami adresów baz danych. Dzięki temu nie jest wymagana konfiguracja pliku TNSNAME.ORA na każdym kliencie.

Oracle Wallet Manager (OWM) może również przechowywać certyfikaty użytkownika. Dzięki tej funkcji użytkownik nie jest związany fizycznie z jednym komputerem.

Integracja z Oracle Single Sign On

Oracle Single Sign On (SSO) to produkt oferujący usługę jednokrotnego logowania.

Serwer SSO sam loguje się serwera OID – posiada specjalne konto. Następnie uwierzytelnia klientów poprzez wyszukanie podanego użytkownika i porównanie jego hasła z przesłanych przez klienta.

Możliwe jest również uwierzytelnianie przez certyfikat klienta. Wówczas serwer SSO porównuje certyfikat przesłany przez klienta z certyfikatem, który znajduje się w OID tego użytkownika.

W zależności od wyniku porównania użytkownik jest uwierzytelniany lub nie.

Integracja z Oracle Portal

Oracle Portal to produkt, który umożliwia tworzenie i zarządzanie portalami. Portal pobiera użytkowników i grupy z serwera OID. Podobnie jak w SSO, Portal wykonuje wyszukiwanie i porównywanie haseł. Portal jest zarejestrowany jako aplikacja podpięta pod zmiany w OID (Provisioning). Oznacza to, że hasło jest sprawdzane tylko raz i zapamiętane w instancji Portalu, a jeśli się zmieni w repozytorium to Portal zostanie o tym powiadomiony.

Uwierzytelnianie użytkowników Portalu może również odbywać się poprzez SSO.

Integracja z Oracle Forms/Reports Services

Oracle Forms i Oracle Reports mogą również wykorzystywać OID do uwierzytelniania użytkowników. Aby włączyć tą funkcjonalność niezbędne jest wykorzystanie serwera SSO.

Wtedy, po udanym uwierzytelnieniu poprzez SSO, serwer Forms/Reports pobiera informacje o zasobach zalogowanego właśnie użytkownika. I na ich podstawie generuje parametr userid, który jest wykorzystywany podczas połączenia formatki/raportu do bazy danych.

Zasoby to wpisy skojarzone z użytkownikiem, które opisują połączenie do bazy danych. Opis połączenia jest definiowalny i może dotyczyć zarówno podłączenia do ORACLE RDBMS, źródeł zewnętrznych Oracle Reports jak i serwera Oracle Express, z którego generowane są raporty. Każdy zasób reprezentowany jest przez nazwę. Nazwa ta jest przekazywana do serwera Forms/Reports jako parametr uruchomieniowy. W zależności od tego parametru pobierany jest odpowiedni zasób.

Dodatkowo aplikacje Forms mogą uzyskać informacja o nazwie użytkownika przez pobranie własności aplikacji SSO_USERID.

Integracja z Oracle Containers for J2EE

Oracle Containers for J2EE (OC4J), do uwierzytelniania i autoryzacji wykorzystuje następujących dostawców:

- XML – oparty o pliki XML, w których nie ma zabezpieczonych haseł
- JAZN-XML – oparty również o plikach XML, ale z zaszyfrowanym hasłem
- JAZN-LDAP – pobiera informacje o użytkownikach z OID

Z uwierzytelnienia JAZN-LDAP mogą korzystać zarówno aplikacje uruchamiane w OC4J jak i aplikacje typu „standalone”.

Integracja z Oracle Internet File System

Oracle Internet File System (IFS) również pobiera informacje o użytkownikach z OID. Dodatkowo rejestruje się jak aplikacja oczekująca powiadomień o zmianach – podobnie jak Oracle Portal.