

Nowości dotyczące bezpieczeństwa w Oracle 10g

Paweł Chomicz (Matrix.pl)

Baza danych Oracle Database 10g podobnie jak jej poprzedniczki zapewnia wysoki poziom bezpieczeństwa. Co więcej wprowadzane w poprzednich wersjach mechanizmy wreszcie zaczynają ze sobą współpracować bez wyrafinowanych zabiegów konfiguracyjnych. Dzięki możliwości integracji z infrastrukturą Identity Management, zapewniono kompleksowe zarządzanie tożsamością, zarządzanie dostępem oraz funkcje wymuszające przestrzeganie zasad bezpieczeństwa. Administratorzy mogą na przykład powierzyć użytkownikom zarządzanie ich hasłami dostępu do bazy danych. Przynosi to korzyści zarówno firmie, w postaci obniżenia kosztów administrowania hasłami, jak i użytkownikom, którzy muszą teraz pamiętać tylko jedno hasło. Aplikacje współpracujące z infrastrukturą Oracle Identity Management mogą korzystać z funkcji bezpieczeństwa oferowanych przez bazę danych Oracle Database 10g, takich jak Fine Grained Audit oraz funkcje standardowe Auditing, Virtual Private Database i Oracle Label Security.

Większość z tych składników rozwijała się od Oracle 8i poprzez 9i jednak dopiero w Oracle 10g osiągnęły one taki stan dojrzałości, że ich konfiguracja oraz użytkowanie nie stanowią już poważnego problemu dla administratorów oraz deweloperów.

Oracle 10g wprowadza w obszarze bezpieczeństwa kilka nowości. Są to między innymi:

- Transparent Data Encryption - pakiet DBMS_CRYPTO jako nowa wersja znanego z Oracle 8i i 9i pakietu DBMS_OBFUSCATION_TOOLKIT;
- Secure Application Roles;
- nowe możliwości w Virtual Private Database;
- Enterprise User Security;
- Proxy Authentication;
- Fine Grained Auditing.

Nowości te same w sobie są interesujące jednak na wykładzie postaram się zaprezentować - poza ich krótkim omówieniem - w jaki sposób dążyc do kompleksowego bezpieczeństwa danych i środowiska ich przetwarzania opartego o Oracle Identity Management.

W dalszej części zaprezentuję składowe Oracle Platform Security:

- Oracle Internet Directory;
- Oracle Directory Integration and Provisioning;
- Oracle Delegated Administration Service;
- Oracle Application Server 10g Single Sign-On;
- Oracle Application Server 10g Certificate Authority.

Cechy ochrony danych w Oracle

Jednokrotne logowanie - do różnych aplikacji eliminuje koszty i ryzyko związane z posiadaniem wielu kont w różnych aplikacjach.

Restrykcyjny dostęp do danych - wirtualna prywatna baza danych (Virtual Private Database) umożliwia uzyskanie bezpiecznego i bezpośredniego dostępu do danych o znaczeniu krytycznym.

Etykiety poufności danych - funkcja Oracle10g Label Security najbardziej ogranicza dostęp do poufnych informacji, poprzez wymuszanie zgodności przywilejów użytkownika z etykietami poufności danych.

Kompleksowa kontrola - funkcje kontroli Oracle10g Auditing pozwalają szybko identyfikować przypadki naruszenia zabezpieczeń i reagować na nie.

Scentralizowane przywileje użytkowników - funkcje Enterprise User Security zintegrowane z usługami LDAP realizują uwierzytelnianie i autoryzację użytkowników.

Szyfrowanie transmisji sieciowej - funkcje Oracle10g Advanced Security obejmują silne szyfrowanie danych transmitowanych siecią oraz ich uwierzytelnianie.

Selektywne szyfrowanie danych w bazie - baza danych Oracle wymusza zachowanie prywatności na najniższym poziomie dostępu do danych.

Obsługa infrastruktury klucza publicznego

Gwarancja - zapewniana przez certyfikaty ocen zabezpieczeń - są one dowodem na to, że Oracle pozostaje liderem pod względem bezpieczeństwa swoich produktów. Na przykład Oracle Label Security posiada Certyfikat International Common Criteria na poziomie EAL4.

Zarządzanie tożsamością - funkcje

Udostępniając dane w trybie online, firma musi radzić sobie z zarządzaniem tożsamością i przywilejami dostępu dla coraz większej liczby użytkowników. Jak zabezpieczyć informacje firmy przed nieautoryzowanym dostępem do systemów i aplikacji o znaczeniu krytycznym? Rozwiązanie Oracle do zarządzania tożsamością (Oracle Identity Management), opracowane z wykorzystaniem nowoczesnej technologii odpornej na ataki, pozwala przygotować infrastrukturę informatyczną do zbudowania sieci grid i zapewnia:

Zgodność - z obowiązującymi przepisami dotyczącymi ochrony danych osobowych (ustawy HIPAA, Gramm-Leach-Bliley, Sarbanes-Oxley) oraz Dyrektywą Unii Europejskiej dotyczącej ochrony danych.

Niższe koszty administrowania - dzięki takim funkcjom, jak: jednokrotne logowanie, automatyczne zarządzanie kontami, przekazywanie przywilejów administracyjnych oraz dzięki mechanizmom samoobsługowym (np. resetowanie haseł lub generowanie certyfikatów cyfrowych).

Większą produktywność użytkowników - dzięki szybszej konfiguracji kont użytkowników oraz integracji z usługami katalogowymi innych producentów.

Większe bezpieczeństwo - dzięki natychmiastowemu odbieraniu przywilejów dostępu po zmianie charakteru współpracy lub jej zakończeniu.

Zarządzanie tożsamością - komponenty

funkcjonalność Identity Management	Komponenty
LDAP directory services	Oracle Internet Directory
Directory integration (meta-directory) oraz Application user provisioning	Oracle Directory Integration and Provisioning
Delegated administration	Oracle Delegated Administration Service
Web single sign-on	Oracle Application Server 10g Single Sign-On
Certificate authority	Oracle Application Server 10g Certificate Authority

Oracle Internet Directory – skalowalne, zgodne z LDAP v3 repozytorium usług katalogowych. Ponieważ jest to podstawowy komponent środowiska Oracle Identity Management został on opisany dokładniej:

Protokół LDAP

LDAP (*Light Weight Directory Access Protocol*) to standard definiujący funkcjonalność katalogu oraz opisujący mechanizmy komunikacji między serwerem a klientem LDAP. Został przewidziany jako okrojona implementacja standardu ISO X.500 definiującego dostęp do usług katalogowych.

Aktualna wersja LDAP v3 została zatwierdzona przez IETF (*Internet Engeneering Task Force*) w 1997 roku. Standard opisany jest

w dokumentach RFC-2251...2256 oraz w innych opublikowanych przez IETF. Jest w pełni zgodna z wersją v2 oraz rozszerza jej funkcjonalność m.in. o:

- Mechanizm odnośników pozwalający na partycjonowanie katalogu.
- Serwer udostępnia klientom schemat katalogu.
- Dopuszcza się stosowanie mechanizmów bezpieczeństwa SASL.

Oracle Internet Directory powstał w oparciu o wersję LDAP v3 i jest z nią w pełni zgodny. Rozszerza jednak funkcjonalność o kilka dodatkowych rozwiązań które nie doczekały się jeszcze standardu, np. bezpieczna autentykacja przy wykorzystaniu SSL.

Usługi katalogowe

Serwer usług katalogowych LDAP jest rodzajem hierarchicznej bazy danych, różni się, więc zasadniczo od modelu relacyjnego. Podstawowe różnice można podzielić na kilka kategorii:

Sposób przechowywania informacji

Baza relacyjna przechowuje informacje w postaci rekordów w tabelach, natomiast dane w katalogu zorganizowane są w postaci wpisów.

Wpisy mogą reprezentować dowolne obiekty, jakimi chcemy zarządzać np.: pracownicy, jednostki organizacyjne, komputery, definicje połączeń sieciowych itd. Każdy wpis posiada atrybuty, którym można przypisać jedną lub więcej wartości.

Atrybuty mają swoje typy. Atrybuty można dowolnie dodawać.

Operowanie na danych

Baza relacyjna zorientowana jest na operacje zapisu. Typowe zastosowanie wiąże się z ciągłym napływem informacji i relatywnie niewielkimi ilościami odczytów. W przypadku katalogu dane są zazwyczaj odczytywane. W typowych zastosowaniach mamy do czynienia z niewielką ilością operacji modyfikacji i bardzo dużą ilością operacji odczytu/wyszukiwania danych.

W przypadku systemów relacyjnych mamy do czynienia z dużymi i zróżnicowanymi transakcjami wykonującymi wiele operacji na dużych ilościach danych. Katalog musi poradzić sobie z względnie prostymi zapytaniami zwracającymi niewielkie ilości danych. Częstym zastosowaniem serwerów katalogowych jest przechowywanie danych teleadresowych. Na przykład aplikacja używa katalogu do odczytu adresów e-mail lub nazwisk użytkowników

Lokalizacja danych

Baza relacyjna może być rozproszona jednak zwykle dane są raczej lokalizowane na jednym serwerze czy też partycji. Natomiast aplikacje korzystające z katalogu spodziewają się znaleźć informacje niezależnie od

serwera, z którym się łączą. Jeżeli dany serwer nie przechowuje informacji lokalnie, powinien zapewnić przekierowanie zapytanie w sposób przezroczysty dla aplikacji.

Podsumowując można powiedzieć, że katalog przypomina bazę danych, ale zawiera bardziej opisowe, oparte na atrybutach informacje. Katalogi nie implementują mechanizmów typowych dla systemów relacyjnych, jak np. transakcje i rollback. Z drugiej jednak strony istnieje konieczność transakcyjności w sensie zachowania spójności danych w ramach całego drzewa wpisów do katalogu. LDAP jest przystosowany do przechowywania niewielkich rekordów w postaci hierarchicznej struktury - bardzo podobnej do drzewiastej struktury katalogów w systemach plików. Usługi katalogowe są łatwo skalowalne - można je dowolnie rozbudowywać w miarę potrzeb - chociażby przez dodawanie kolejnych maszyn obsługujących poszczególne "gałęzie" drzewa LDAP.

Budowa katalogu

Poniżej podano definicje podstawowych elementów tworzących katalog oraz terminów związanych z katalogami.

Drzewo Katalogu DIT (Directory Information Tree) - Informacje w katalogu posiadają strukturę drzewiastą, najczęściej odzwierciedlającą podziały geograficzne i organizacyjne. Wpisy zorganizowane są w tzw. Drzewo Katalogu. Możemy wyróżnić „gałęzie”, czyli obiekty zawierające inne obiekty oraz „liście” czyli wpisy końcowe.

Wpis (entry) - Wpis to zbiór informacji o dowolnym obiekcie w katalogu zorganizowanych w atrybuty. Każdy wpis jest w sposób jednoznaczny identyfikowany przez nazwę pełną. Podstawowym i pierwszym wpisem w drzewie DIT jest korzeń (root) DSE (*Directory Specific Entry*).

Nazwa Pełna DN (Distinguished Name) - Nazwa Pełna zawiera dokładną lokalizację wpisu w drzewie katalogu, a więc listę wpisów które prowadzą do danego obiektu w drzewie. DSE jest identyfikowany przez pusty ciąg „”.

Atrybuty - Każdy wpis składa się z atrybutów, które przechowują wartości (dane). Każdy atrybut posiada nazwę oraz wartość określonego i zdefiniowanego typu. Niektóre atrybuty mogą być wielowartościowe, co pozwala na lepsze oddanie opisywanej rzeczywistości. Przykładowo osoba może posiadać więcej niż jeden numer telefonu.

Klasa - Klasa opisuje strukturę wpisu, informuje o tym, jakie atrybuty może, a jakie musi zawierać dany wpis. Nowe klasy można definiować jako podklasy klas istniejących. Podklasa dziedziczy wszystkie atrybuty klasy nadrzędnej. Wszystkie klasy w katalogu są podrzędne dla klasy top,

dlatego każdy wpis musi do niej należeć. Każdy wpis musi posiadać atrybut `objectClass`, który przechowuje nazwy klas do których należy opisywany obiekt.

Atrybuty obowiązkowe - Jeżeli klasa posiada atrybuty obowiązkowe, wpis nie może należeć do tej klasy i jednocześnie nie mieć określonej wartości dla tych atrybutów.

Atrybuty opcjonalne - Atrybuty określone dla klasy jako opcjonalne mogą lecz nie muszą mieć ustalonych wartości we wpisie.

Atrybuty operacyjne - Atrybuty operacyjne (systemowe) nie zawierają danych aplikacyjnych lecz informacje uzupełniane i w pełni zarządzane przez serwer katalogowy. OID implementuje cztery atrybuty operacyjne:

creatorsName – pełna nazwa twórcy wpisu w katalogu;

createTimestamp – czas stworzenia wpisu;

modifiersName – pełna nazwa użytkownika który ostatnio modyfikował wpis;

modifyTimestamp – czas ostatniej modyfikacji.

Atrybuty operacyjne nie są wyświetlane w wyniku zwykłego wyszukiwania, nawet jeśli dotyczy ono wszystkich atrybutów. Aby wyświetlić wartość jednego z atrybutów operacyjnych trzeba jawnie podać jego nazwę podczas wyszukiwania.

Nazwany kontekst

Nazwany kontekst (naming context) to poddrzewo znajdujące się w całości na jednym serwerze. Musi być ciągłe, to znaczy musi zaczynać się od jednego wpisu (szczytu poddrzewa) i rozszerzać w dół aż do ostatnich wpisów (liści) lub do odnośników. Może obejmować zarówno jeden wpis jak i całe drzewo. Podstawowy wpis będący korzeniem drzewa (root DSE) nie jest częścią żadnego nazwanego kontekstu.

Wydzielone nazwane konteksty można publikować aby umożliwić użytkownikom ich wyszukiwanie.

Schemat

Zbiór informacji opisujących dozwolone struktury danych w obrębie katalogu. Zawiera definicje typów atrybutów, definicje klas oraz informacje potrzebne do określenia reguł porównywania wartości atrybutów.

Definicja schematu dla całego drzewa w OID 3.0 przechowywana jest w atrybutach specjalnego wpisu: `cn=subschemaSubentry`. Modyfikując atrybuty w tym wpisie można zmieniać definicje klas, atrybutów itd. Oracle nie zaleca ręcznej modyfikacji schematu, do tego celu należy stosować narzędzie *Oracle Directory Manager*.

Oracle Directory Integration

Przedsiębiorstwa często wykorzystują wiele rozwiązań, systemów informatycznych, do różnych zastosowań. Przykładowo te same informacje dotyczące pracowników mogą być przechowywane w bazie HR, systemie pocztowym, w różnych aplikacjach do których pracownicy mają dostęp. Prowadzi to do redundancji danych a co z tym idzie, do problemów z utrzymaniem spójności informacji oraz narzutu na administrowanie wieloma systemami.

Rozwiązaniem tych problemów może być **metekatalog**. Metakatalogiem nazywamy rozwiązanie które pozwoli na synchronizację informacji przechowywanych w różnych miejscach z jednym katalogiem centralnym, łącząc wszystkie informacje w jeden wirtualny katalog. Stosując metakatalog można zcentralizować zarządzanie danymi co znacznie zredukuje koszty administracyjne nie rezygnując z wykorzystania dotychczasowych wyspecjalizowanych katalogów.

Oracle Internet Directory może spełniać funkcje metakatalogu dla dowolnego środowiska, w którym działają gotowe wyspecjalizowane katalogi. Rozwiązanie firmy Oracle nosi nazwę Platformy Integracyjnej i działa w oparciu o technologię OID.

Platforma Integracyjna pozwala na synchronizację danych z dowolnego zewnętrznego źródła z centralnym katalogiem OID. Synchronizacja jest możliwa w obie strony, zmiany wprowadzone w OID mogą być propagowane do odpowiednich katalogów zewnętrznych, zmiany wprowadzone w zewnętrznych katalogach przy pomocy charakterystycznych dla nich aplikacji klienckich, mogą być aplikowane do centralnego katalogu OID.

Platforma Integracyjna działa w oparciu o następujące komponenty:

Katalogi Zewnętrzne

Niezależne źródła informacji - bazy danych - dla których OID będzie katalogiem centralnym, można nazwać katalogami zewnętrznymi. Mogą nimi być na przykład: bazy relacyjne, Microsoft Exchange, Lotus Notes, Oracle HR, lub dowolne inne źródło dla którego istnieje opisany interfejs wymiany informacji.

Oracle Internet Directory

Serwer katalogowy przechowujący dane w relacyjnej bazie Oracle9i. Spełnia rolę centralnego katalogu przechowującego wszystkie informacje oraz dostarcza standardowego interfejsu dostępu do danych (protokół LDAP).

Katalog centralny OID może być fizycznie replikowany między kilkoma serwerami, jednak replikacja między węzłami OID jest realizowana przy pomocy znacznie bardziej wydajnych mechanizmów opisanych wcześniej.

Serwer Integracyjny (Oracle Directory Integration Server)

Podobnie jak w przypadku serwera katalogowego czy replikacyjnego, OID pozwala na uruchomienie instancji serwera integracyjnego. Serwer integracyjny to wielowątkowy proces odpowiedzialny za:

- Kontrolowanie pracy agentów integracyjnych
- Wykonywanie konwersji danych na podstawie reguł ustalonych dla każdego katalogu zewnętrznego
- Obsługę błędów

Odpowiedni wpis konfiguracyjny, określa sposób zachowania instancji serwera integracyjnego oraz listę kontrolowanych agentów integracyjnych.

Agent Integracyjny (Directory Integration Agent)

Agent integracyjny to program odpowiedzialny za faktyczne przekazywanie danych między OID a katalogiem zewnętrznym i odwrotnie. Może działać pod nadzorem serwera integracyjnego, wtedy serwer uruchamia agenta w określonych odstępach czasowych, wykonuje konwersję danych (które atrybuty i w jaki sposób przekazać agentowi), jeśli trzeba aplikuje również dane dostarczone przez agenta.

Mogą istnieć również agenci niezależni od platformy integracyjnej niekontrolowani przez serwer integracyjny lecz inny zewnętrzny metakatalog.

Pliki Eksportu / Importu

Wymiana informacji między serwerem integracyjnym a agentami odbywa się poprzez pliki eksportu i importu. Pliki eksportu opisują zmiany które należy przekazać do katalogu zewnętrznego, pliki importu opisują zmiany propagowane z katalogu zewnętrznego do OID.

Informacje dotyczące konfiguracji agentów mogą być przechowywane w katalogu OID, w specjalnym atrybucie określającym tak zwany profil integracyjny. Wartość tego argumentu jest przekazywana agentowi w momencie jego uruchamiania.

Dla każdego zewnętrznego katalogu musi istnieć zestaw reguł (Mapping Rules) określających które atrybuty i w jaki sposób tłumaczyć. Serwer integracyjny odczytuje te reguły i stosuje je podczas eksportowania lub importowania danych z konkretnego katalogu zewnętrznego.