

Virtual Private Database

Paweł Chomicz (Matrix.pl)

Virtual Private Database jest wprowadzonym w Oracle8i mechanizmem umożliwiającym separację danych na poziomie serwera bazy danych oraz ustalanie praw dostępu do danych z granulacją do wiersza. VPD umożliwia zatem powiązanie praw dostępu do danych w tabelach z hierarchiczną strukturą organizacyjną firmy bez konieczności implementacji dodatkowych mechanizmów separacji użytkowników w systemach transakcyjnych oraz raportowych.

Podstawową zaletą takiego rozwiązania jest uniezależnienie praw dostępu do wierszy od sposobu sięgania po dane. Dostęp użytkownika do serwera poprzez aplikacje czy też bezpośrednio przez SQL/Plus da taki sam efekt: odpowiednie dane będą nie widoczne. Prawdę mówiąc użytkownik w ogóle nie będzie sobie zdawał sprawy z tego, że pewne dane są dla niego niedostępne.

Drugą zaletą to możliwość naturalnego przechowywania logicznie powiązanych informacji w pojedynczych tabelach lub ich grupach bez dodatkowego, sztucznego znakowania wierszy.

Mechanizm VPD oparty został o przypisanie do tabel kolumn zawierających etykiety opisujące pewne reguły dostępu oraz przypisanie do użytkowników uprawnień odpowiadających tym regułom. Decyzja co do tego czy użytkownik może odczytać wiersz danych z tabeli oraz czy może wykonać na nim inne operacje jest podejmowana przez porównanie bitowych reprezentacji tych reguł i uprawnień.

Są trzy podstawowe klasy reguł:

poziomy – level;
przegródki – compartment;
grupy – group.

Taka logika umożliwia budowanie złożonych reguł dostępu do danych.

Poziomy zapewniają liniowy dostęp hierarchiczny. Osoba uprawniona po poziomie wyższego ma również dostęp do poziomu niższego. Bardzo dobrze odpowiada to na przykład prawom do zatwierdzania wydatków. Poziomy nie mogą być od siebie zależne inaczej niż liniowo.

Grupy umożliwiają z kolei ustalanie praw hierarchicznych. Kilka grup może podlegać jednej grupie a ona z kolei innej. Bardzo dobrze odpowiada to strukturze organizacyjnej firmy lub podziałowi terytorialnemu. Ostatnie **przegródki** ustalają już prawa bez hierarchii i poziomów. Do konkretnej przegródki ma się prawo albo go się nie ma.

Dostęp do OLS został zrealizowany przez:
API – bardzo rozbudowany interfejs w PL/SQL;
OCI – niskopoziomowy interfejs dla programistów;
Oracle Policy Managera – środowisko graficzne dla administratorów.

Reguły mogą być przypisane do: tabel, widoków oraz synonimów (za wyjątkiem polityki wskazującej określoną kolumnę – Column-Level).

Możliwe jest również audytowanie różnych operacji użytkowników.

W Oracle9i został dodany mechanizm Oracle Label Security który jest rozszerzeniem VPD umożliwiającym łatwiejsze niż w VPD zarządzanie prawami użytkowników.

W Oracle10g mechanizm Virtual Private Database został rozbudowany o:

1. statyczne, szybkie polityki bezpieczeństwa oraz dzielenie różnych polityk bezpieczeństwa dla tego samego obiektu;

W Oracle9i były zaimplementowane jedynie dynamiczne polityki bezpieczeństwa, to znaczy funkcje które były każdorazowo wołane przy każdym dostępie do tabeli.

Oracle10g wprowadza polityki statyczne:

Tym obiektu	Typy statyczne	Typy dynamiczne
Single Object	Static	Dynamic Context_Sensitive
Multiple Objects	Shared_Static	Shared_Context_Sensitive

Static – funkcja wyliczająca predykat jest wyliczana jeden raz, wynik jest umieszczany i przechowywany w SGA;

Dynamic – odpowiednik polityk Oracle9i;

Context_Sensitive – funkcja wyliczająca predykat jest wołana tylko wtedy kiedy zmienia się kontekst aplikacji; ma to zastosowanie głównie do aplikacji Internetowych;

Shared_Static oraz **Shared_Context_Sensitive** – to samo co Static oraz, odpowiednio Context_Sensitive tylko dla wielu obiektów; na przykład tabel połączonych referencją o ile funkcja wyliczająca predykat dotyczy pól określających referencje.

2. określenie polityki bezpieczeństwa w zależności od kolumn na których wykonywane są zapytania;

W polityce bezpieczeństwa można zdecydować, że dana polityka będzie włączana jedynie wtedy kiedy w zapytaniu odnoszącym się do określonej tabeli czy widoku w sposób jawny lub nie jawny nastąpi odwołanie do konkretnej kolumny określonej w polityce. W pozostałych przypadkach, to znaczy wtedy kiedy w zapytaniu w żaden sposób nie nastąpi odwołanie do tej kolumny polityka nie będzie włączana.

3. integracja z Oracle Identity Management;
4. użycie Virtual Private Database dla zapytań równoległych.

Plan warsztatu:

1. Historia VPD.
2. Nowe cechy VPD.
3. Instalacja i konfiguracja VPD i OLS.
4. Pakiet biblioteczny dbms_ols.
5. Prezentacja przykładowej aplikacji automatyzującej proces przepisania praw dostępu z hierarchii firmy.