

VIII Seminarium PLOUG
Warszawa
Kwiecień 2003

Oracle Label Security

Paweł Chomicz

(chomicz@alkom.com.pl)

Altkom Akademia S.A.

1. Wstęp

Artykuł został opracowany na podstawie materiału zawartego pod adresem: <http://www.oracle-base.com/Articles/9i/OracleLabelSecurity9i.asp> oraz na podstawie dokumentacji Oracle Label Security Administrator's Guide Release 2 (9.2).

Mechanizm Oracle Label Security jest rozszerzeniem mechanizmu Virtual Private Database prowadzonego w 8i wersji Oracle.

Mechanizm OLS umożliwia łatwiejsze niż w VPD zarządzanie dostępem użytkowników do danych z granulacją do poszczególnych wierszy.

Mechanizm 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 przegrodki ma się prawo albo go się nie ma.

Dostęp do OLS został zrealizowany przez:

API – bardzo rozbudowany interfejs w PL/SQL;

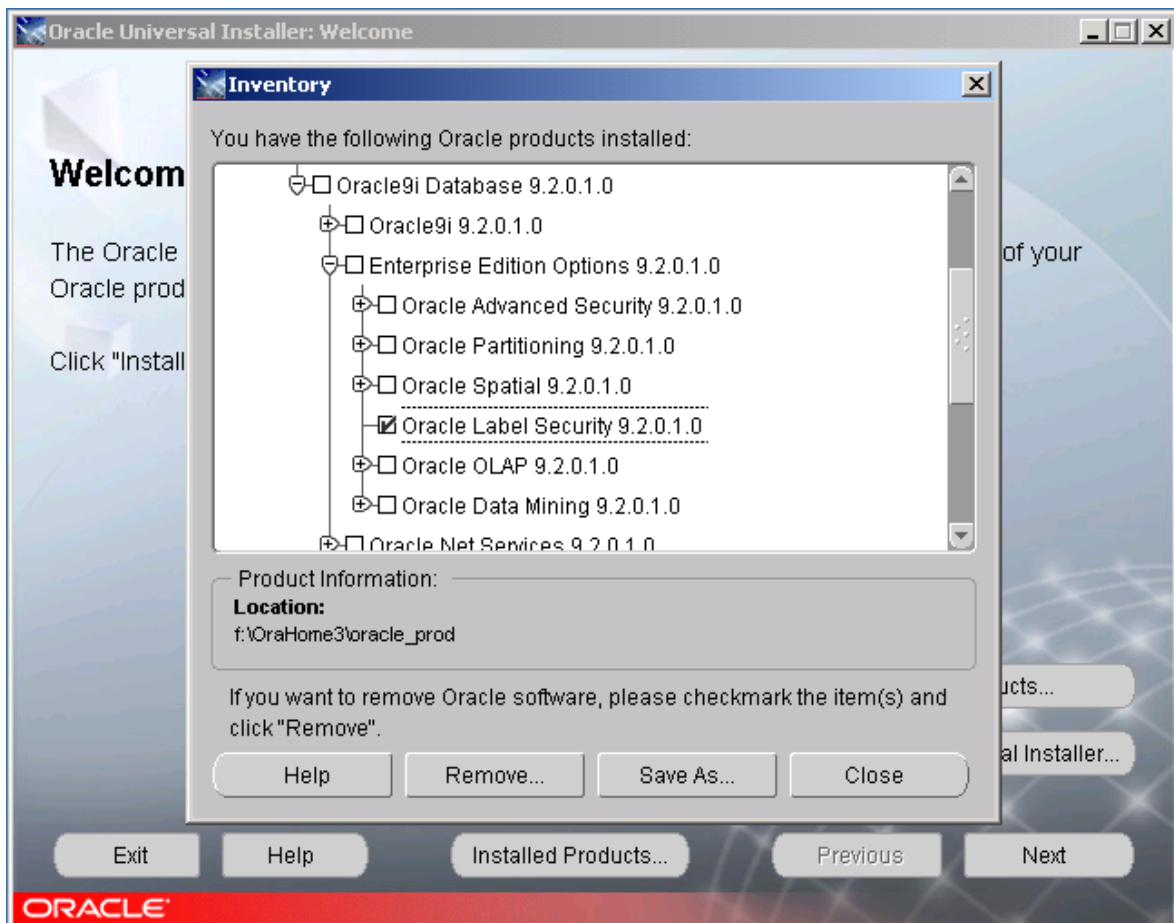
OCI – niskopoziomowy interfejs dla programistów;

Oracle Policy Managera – środowisko graficzne dla administratorów.

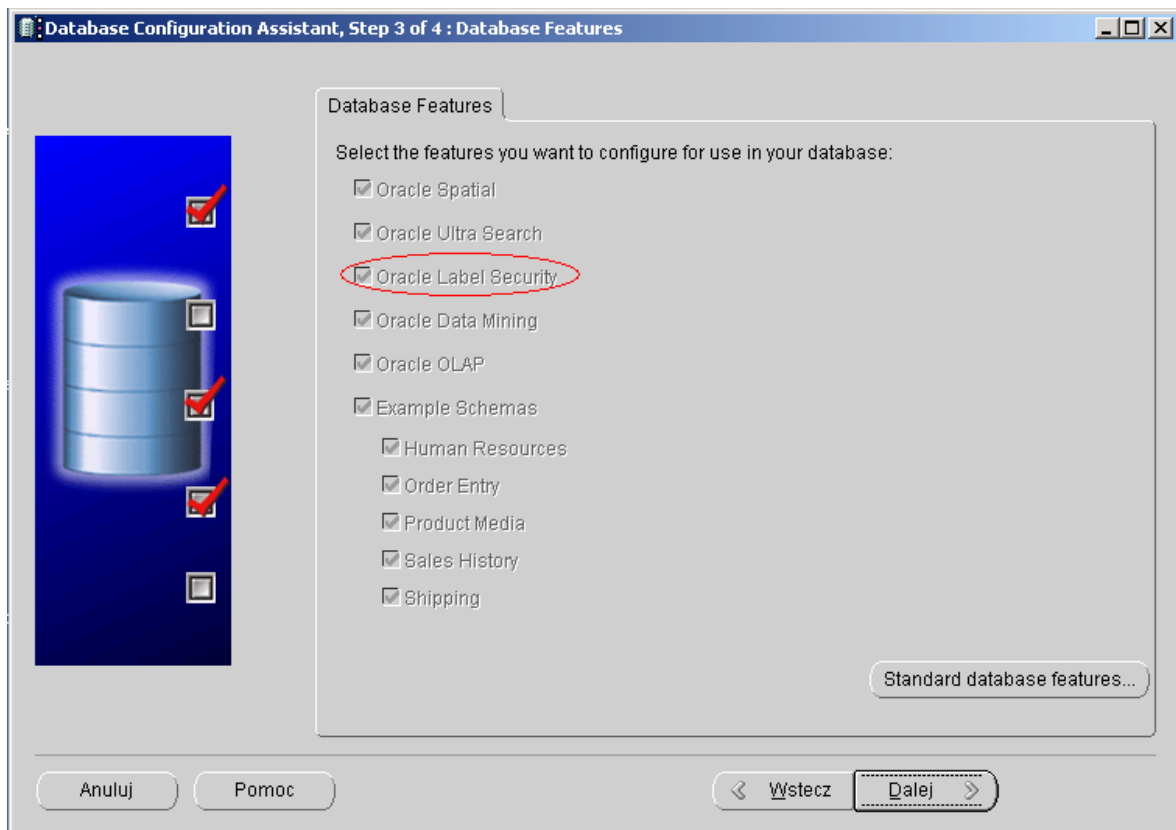
Możliwe jest również audytowanie różnych operacji użytkowników.

2. Instalacja i konfiguracja bazy danych

- Uruchomić instalator Oracle (OUI).
- Na formatce Welcome nacisnąć przycisk Next.
- Wskazać właściwą ścieżkę do źródeł oprogramowania, wybrać właściwy Oracle Home następnie nacisnąć przycisk Next.
- Wybrać instalację Oracle9i Database i nacisnąć przycisk Next.
- Wybrać instalację typu Custom nacisnąć przycisk Next.
- W gałęci Enterprise Edition Options zaznaczyć opcję Oracle Label i nacisnąć przycisk Next.
- Na formularzu Summary nacisnąć przycisk Install.
- Po informacji o poprawnym zakończeniu instalacji zakończyć działanie OUI.



- Uruchomić Database Configuration Assistant (DBCA).
(Start -> Programs -> Oracle - 92010 -> Configuration and Migration Tools -> Database Configuration Assistant)
- Na formularzu Welcome nacisnąć przycisk Install.
- Na formularzu Operations wybrać opcję "Configure database options in a database" i nacisnąć przycisk Next.
- Na formularzu Databases wybrać właściwą instancję i nacisnąć przycisk Next.
- Na formularzu Database Features upewnić się, że jest wybrana opcja Oracle Label Security i nacisnąć przycisk Next.
- Nacisnąć przycisk Finish.
- Po zakończeniu operacji należy zakończyć pracę Asystenta Konfiguracji Bazy danych, położyć i podnieść instancję bazy danych.



3. Utworzenie użytkownika który będzie zarządzał prawami do danych w swoim chemacie.

```
CREATE USER ols IDENTIFIED BY ols DEFAULT TABLESPACE users TEMPORARY
TABLESPACE temp;
```

```
GRANT CONNECT, RESOURCE, SELECT_CATALOG_ROLE TO ols;
```

```
CONNECT lbacsys/lbacsys
```

```
GRANT EXECUTE ON sa_components TO ols WITH GRANT OPTION;
GRANT EXECUTE ON sa_user_admin TO ols WITH GRANT OPTION;
GRANT EXECUTE ON sa_user_admin TO ols WITH GRANT OPTION;
GRANT EXECUTE ON sa_label_admin TO ols WITH GRANT OPTION;
GRANT EXECUTE ON sa_policy_admin TO ols WITH GRANT OPTION;
GRANT EXECUTE ON sa_audit_admin TO ols WITH GRANT OPTION;
```

```
GRANT LBAC_DBA TO ols;
GRANT EXECUTE ON sa_sysdba TO ols;
GRANT EXECUTE ON to_lbac_data_label TO ols;
```

```
CONNECT ols/ols
```

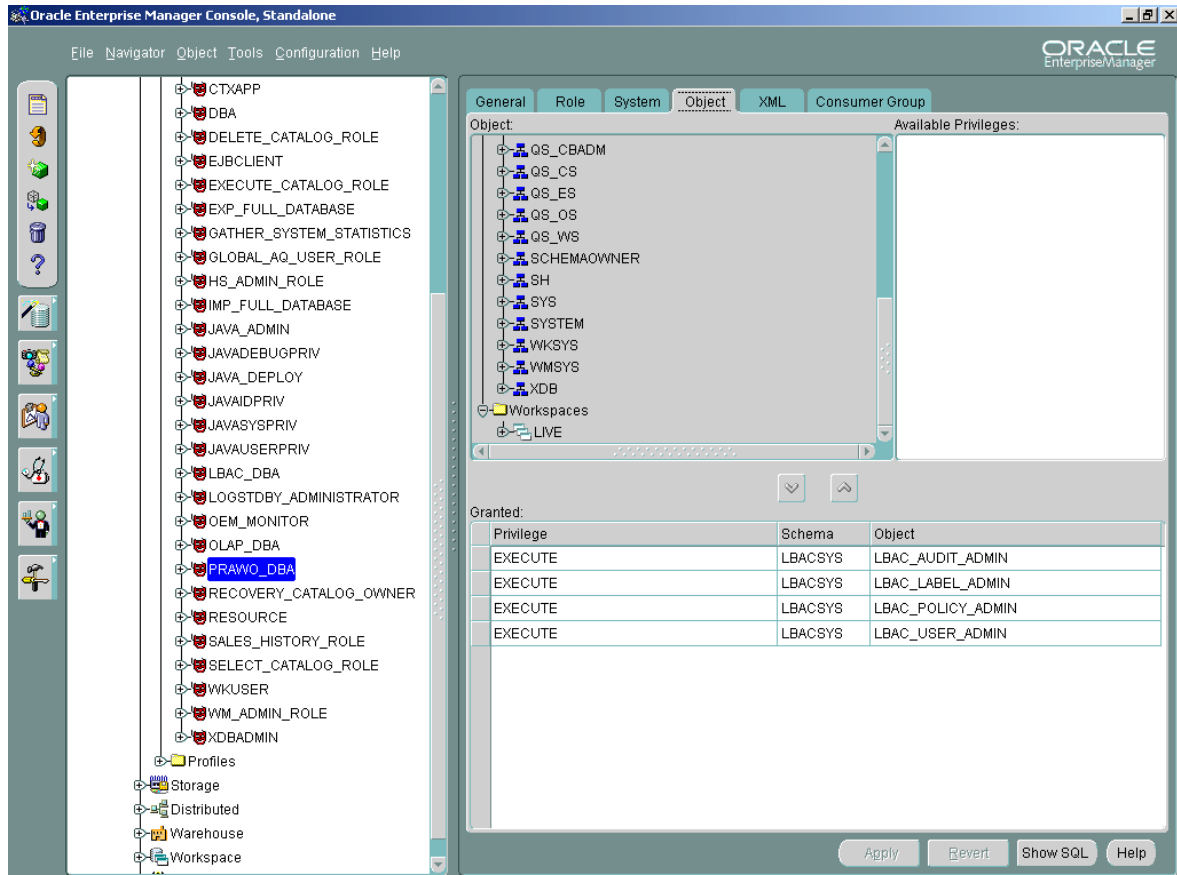
4. Utworzenie etykiety bezpieczeństwa

```
BEGIN
  SA_SYSDBA.CREATE_POLICY (
```

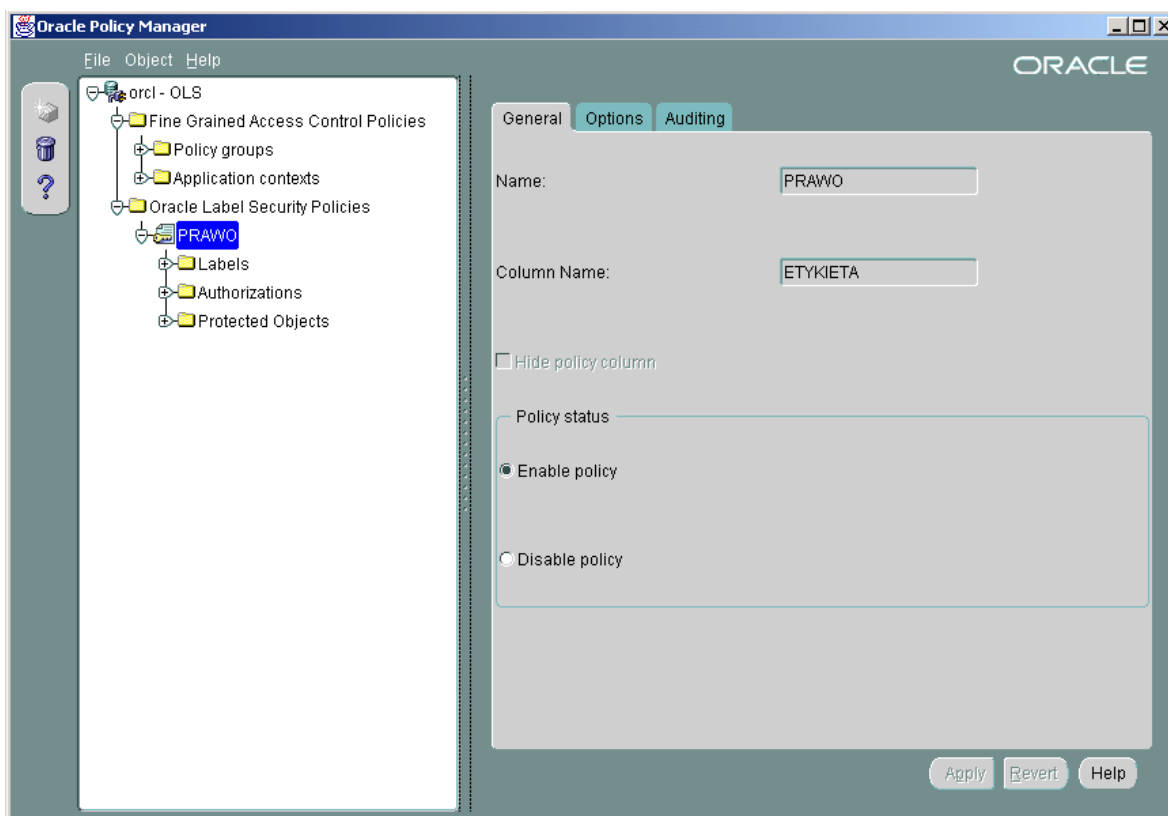
```

policy_name => 'prawo',
column_name => 'etykieta');
END;
/

```

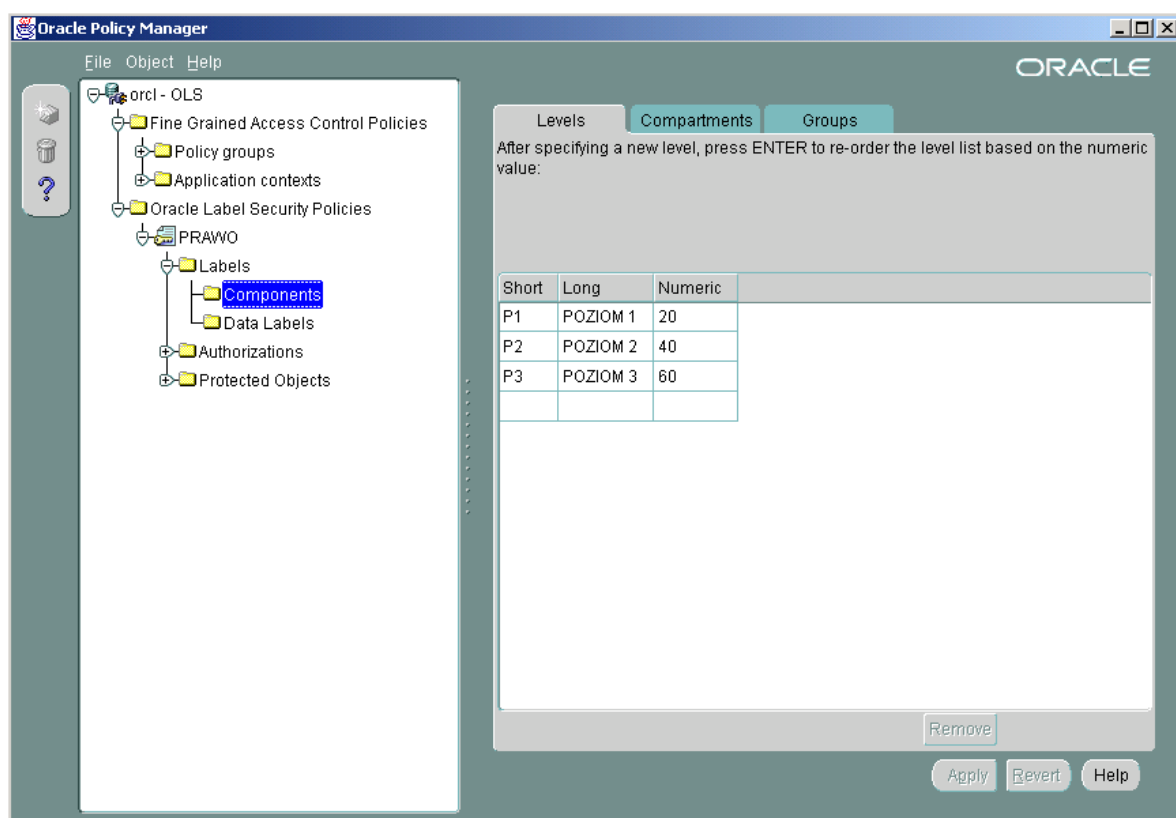


```
GRANT prawo_DBA TO ols;
```



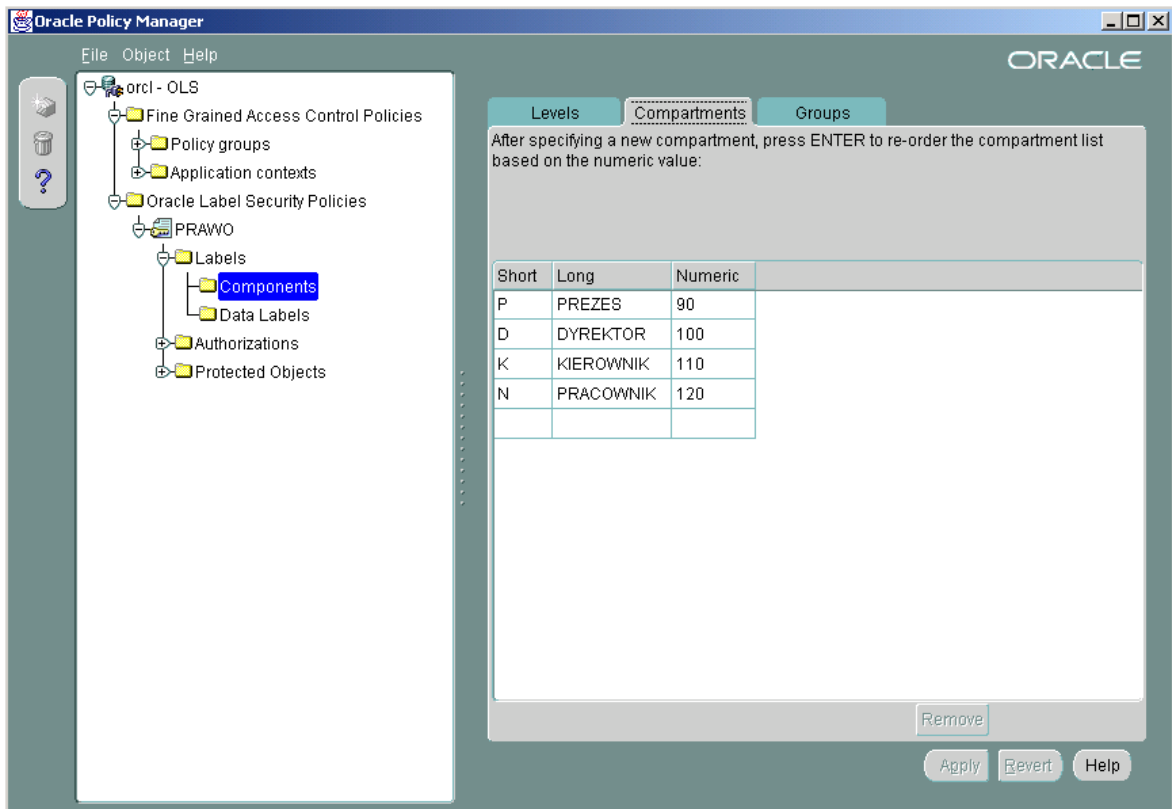
5. Przypisanie do etykiety bezpieczeństwa poziomów dostępu

```
EXECUTE SA_COMPONENTS.CREATE_LEVEL('prawo',20,'P1','Poziom 1');  
EXECUTE SA_COMPONENTS.CREATE_LEVEL('prawo',40,'P2','Poziom 2');  
EXECUTE SA_COMPONENTS.CREATE_LEVEL('prawo',60,'P3','Poziom 3');
```



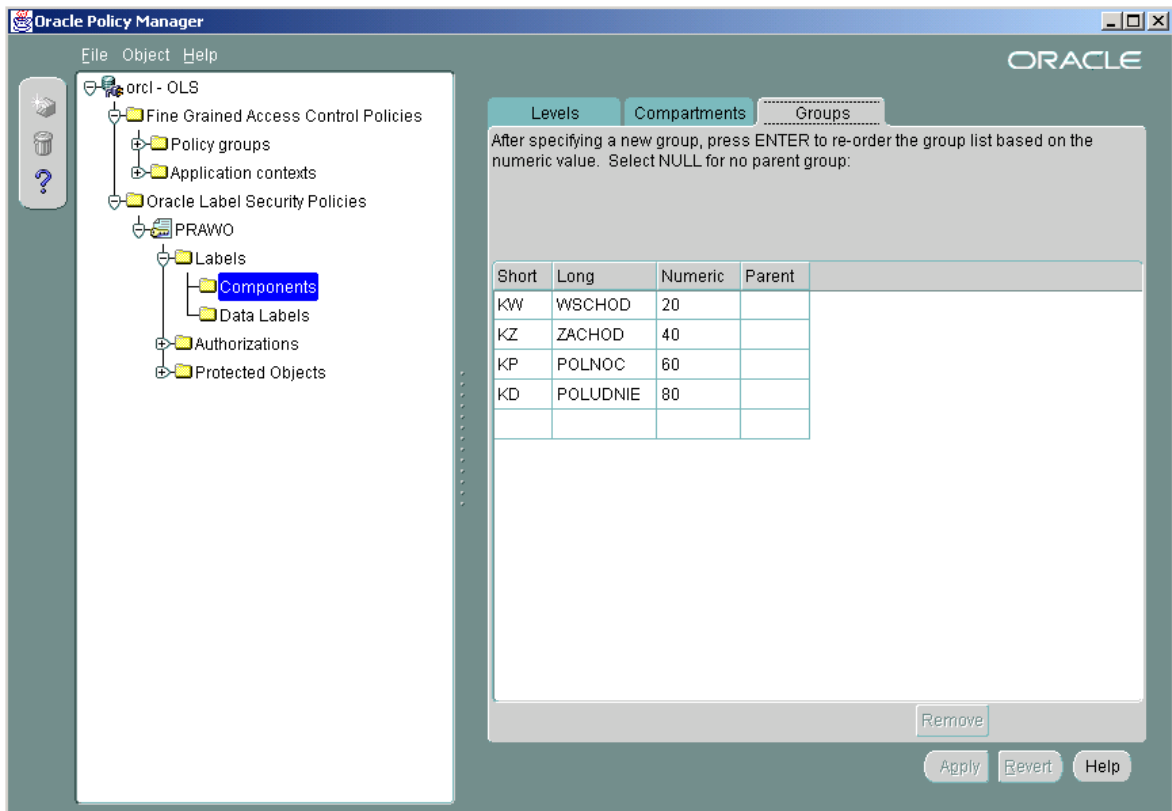
6. Przepisanie do etykiety bezpieczeństwa przegródek

```
EXECUTE SA_COMPONENTS.CREATE_COMPARTMENT('prawo',90,'P','PREZES');  
EXECUTE SA_COMPONENTS.CREATE_COMPARTMENT('prawo',100,'D','DYREKTOR');  
EXECUTE SA_COMPONENTS.CREATE_COMPARTMENT('prawo',110,'K','KIEROWNIK');  
EXECUTE SA_COMPONENTS.CREATE_COMPARTMENT('prawo',120,'N','PRACOWNIK');
```

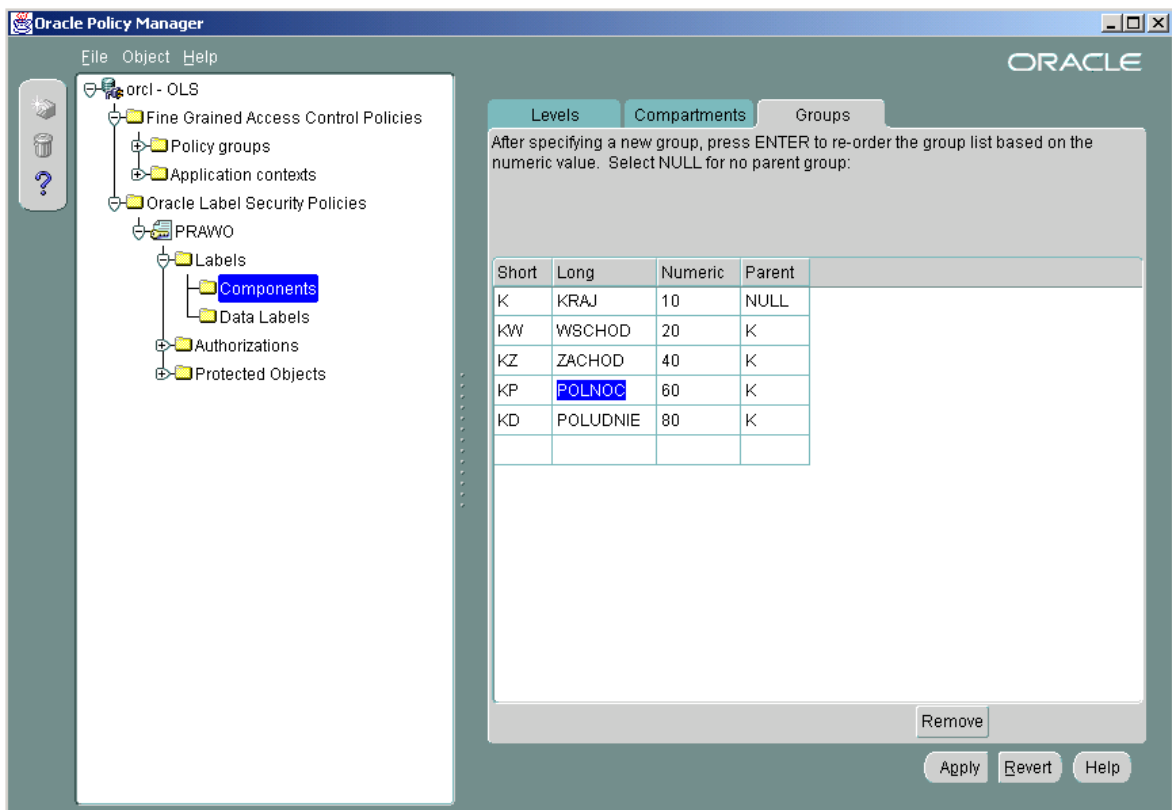


7. Przypisanie do etykiety bezpieczeństwa grup hierarchicznych

```
EXECUTE SA_COMPONENTS.CREATE_GROUP('prawo',20,'KW','WSCHOD');
EXECUTE SA_COMPONENTS.CREATE_GROUP('prawo',40,'KZ','ZACHOD');
EXECUTE SA_COMPONENTS.CREATE_GROUP('prawo',60,'KP','POLNOC');
EXECUTE SA_COMPONENTS.CREATE_GROUP('prawo',80,'KD','POLUDNIE');
```



```
EXECUTE SA_COMPONENTS.CREATE_GROUP('prawo',10,'K','KRAJ');
```



```
EXECUTE
SA_USER_ADMIN.SET_USER_PRIVS('prawo','ols','FULL,PROFILE_ACCESS');

CONNECT ols/ols
```

8. Utworzenie tabeli sprzedawcy

```
CREATE TABLE sprzedawcy (
  id                NUMBER(10) NOT NULL,
  rodzaj_klienta   VARCHAR2(10),
  imie              VARCHAR2(30),
  nazwisko          VARCHAR2(30),
  region            VARCHAR2(10),
  kredyt            NUMBER(10,2),
  CONSTRAINT klienci_pk PRIMARY KEY (id));

GRANT SELECT, INSERT, UPDATE, DELETE ON sprzedawcy TO PUBLIC;
```

9. Zasilenie tabeli sprzedawcy danymi testowymi

```
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
  VALUES ( 1, 'srebrny', 'Pawel', 'Bik', 'WSCHOD', 11000.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
  VALUES ( 2, 'srebrny', 'Jacek', 'Gigola', 'WSCHOD', 2000.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
  VALUES ( 3, 'srebrny', 'Anna', 'Bajor', 'ZACHOD', 500.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
  VALUES ( 4, 'srebrny', 'Pawel', 'Bialy', 'POLUDNIE', 1000.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
  VALUES ( 5, 'srebrny', 'Robert', 'Uprzejmy', 'POLNOC', 20000.00);

INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
  VALUES ( 6, 'zloty', 'Alicja', 'Lopez', 'ZACHOD', 500.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
  VALUES ( 7, 'zloty', 'Katarzyna', 'Broszka', 'WSCHOD', 1000.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
  VALUES ( 8, 'zloty', 'Maria', 'Drop', 'ZACHOD', 1000.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
  VALUES ( 9, 'zloty', 'Dani', 'Minogue', 'POLUDNIE', 20000.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
  VALUES (10, 'zloty', 'Anna', 'Jopek', 'POLNOC', 500.00);

INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
```

```

VALUES (11, 'platynowy', 'Adam', 'Ec', 'POLUDNIE', 500.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
VALUES (12, 'platynowy', 'Anna', 'Klucha', 'WSCHOD', 2000.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
VALUES (13, 'platynowy', 'Ewa', 'Prasna', 'ZACHOD', 10000.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
VALUES (14, 'platynowy', 'Dariusz', 'Bobik', 'POLNOC', 2000.00);
INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
VALUES (15, 'platynowy', 'Jan', 'Wstretny', 'POLNOC', 100.00);

INSERT INTO sprzedawcy (id, rodzaj_klienta, imie, nazwisko, region,
kredyt)
VALUES (50, 'diamentowy', 'Iwan', 'Grozny', 'KRAJ', 100000.00);

COMMIT;

```

10. Utworzenie funkcji tworzącej odpowiednie wpisy etykiety bezpieczeństwa

```

CREATE OR REPLACE FUNCTION get_sprzedawca_label (
  p_rodzaj_klienta IN VARCHAR2,
  p_region        IN VARCHAR2,
  p_kredyt        IN NUMBER)
RETURN LBACSYS.LBAC_LABEL AS
  v_label VARCHAR2(80);
BEGIN
  IF p_kredyt > 2000 THEN
    v_label := 'P3: ';
  ELSIF p_kredyt > 500 THEN
    v_label := 'P2: ';
  ELSE
    v_label := 'P1: ';
  END IF;

  IF p_rodzaj_klienta = 'diamentowy' THEN
    v_label := v_label || 'P: ';
  ELSIF p_rodzaj_klienta = 'platynowy' THEN
    v_label := v_label || 'D: ';
  ELSIF p_rodzaj_klienta = 'pzloty' THEN
    v_label := v_label || 'K: ';
  ELSIF p_rodzaj_klienta = 'srebrny' THEN
    v_label := v_label || 'N: ';
  END IF;

  IF p_region = 'WSCHOD' THEN
    v_label := v_label || 'KW';
  ELSIF p_region = 'ZACHOD' THEN
    v_label := v_label || 'KZ';
  ELSIF p_region = 'POLNOC' THEN
    v_label := v_label || 'KP';
  ELSIF p_region = 'POLUDNIE' THEN
    v_label := v_label || 'KD';
  END IF;

```

```

ELSIF p_region = 'KRAJ' THEN
  v_label := v_label || 'K';
END IF;

RETURN TO_LBAC_DATA_LABEL('prawo',v_label);
END get_sprzedawca_label;
/

SHOW ERRORS

connect ols/ols

```

11. Przypisanie etykiety bezpieczeństwa do tabelo

```

BEGIN
  SA_POLICY_ADMIN.APPLY_TABLE_POLICY (
    policy_name => 'prawo',
    schema_name => 'OLS',
    table_name => 'sprzedawcy',
    table_options => 'NO_CONTROL');
END;
/

UPDATE sprzedawcy
SET etykieta = CHAR_TO_LABEL('prawo','P1');

```

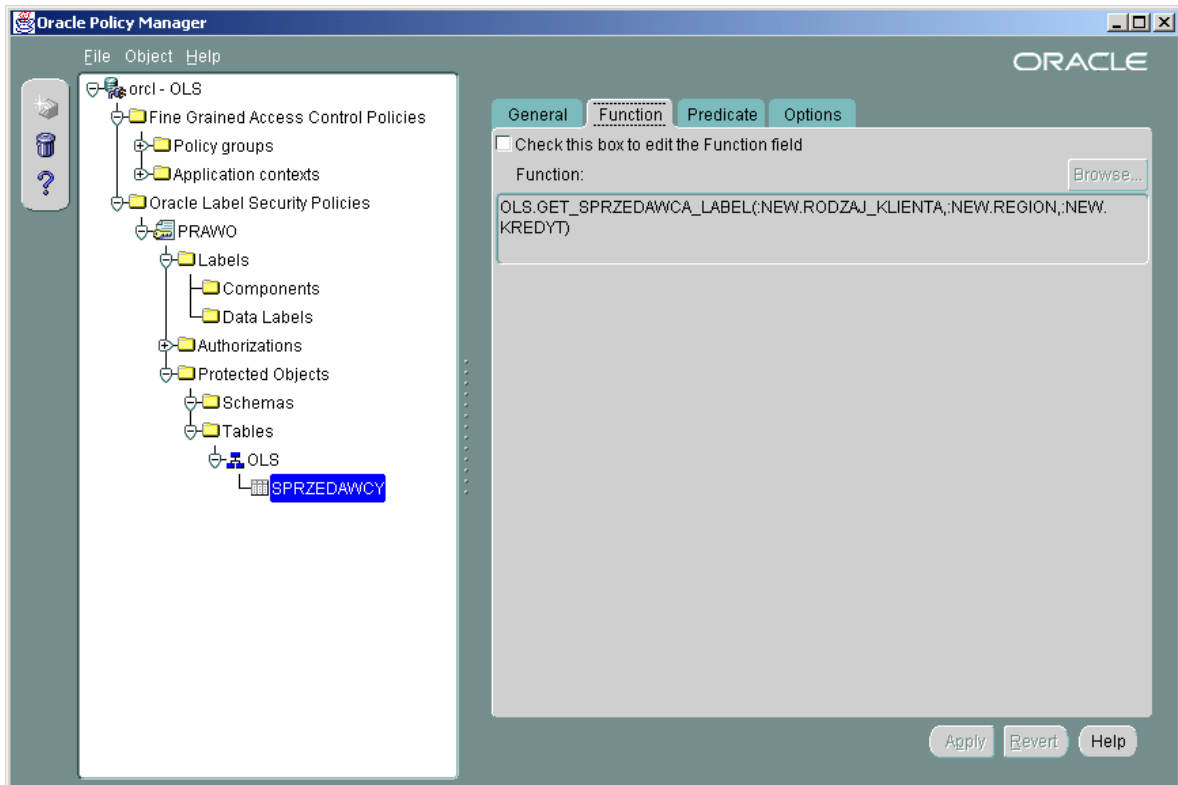
ID	RODZAJ_KLIENTA	IMIE	NAZWISKO	REGION	KREDYT	ETYKIETA
1	srebrny	Pawel	Bik	WSCHOD	11000	1000000060
2	srebrny	Jacek	Gigola	WSCHOD	2000	1000000060
3	srebrny	Anna	Bajor	ZACHOD	500	1000000060
4	srebrny	Pawel	Bialy	POLUDNIE	1000	1000000060
5	srebrny	Robert	Uprzejmy	POLNOC	20000	1000000060
6	zloty	Alicja	Lopez	ZACHOD	500	1000000060
7	zloty	Katarzyna	Broszka	WSCHOD	1000	1000000060
8	zloty	Maria	Drop	ZACHOD	1000	1000000060
9	zloty	Dani	Minogue	POLUDNIE	20000	1000000060
10	zloty	Anna	Jopek	POLNOC	500	1000000060
11	platynowy	Adam	Ec	POLUDNIE	500	1000000060
12	platynowy	Anna	Klucha	WSCHOD	2000	1000000060
13	platynowy	Ewa	Prasna	ZACHOD	10000	1000000060
14	platynowy	Dariusz	Bobik	POLNOC	2000	1000000060
15	platynowy	Jan	Wstretny	POLNOC	100	1000000060
50	diamentowy	Iwan	Grozny	KRAJ	100000	1000000060

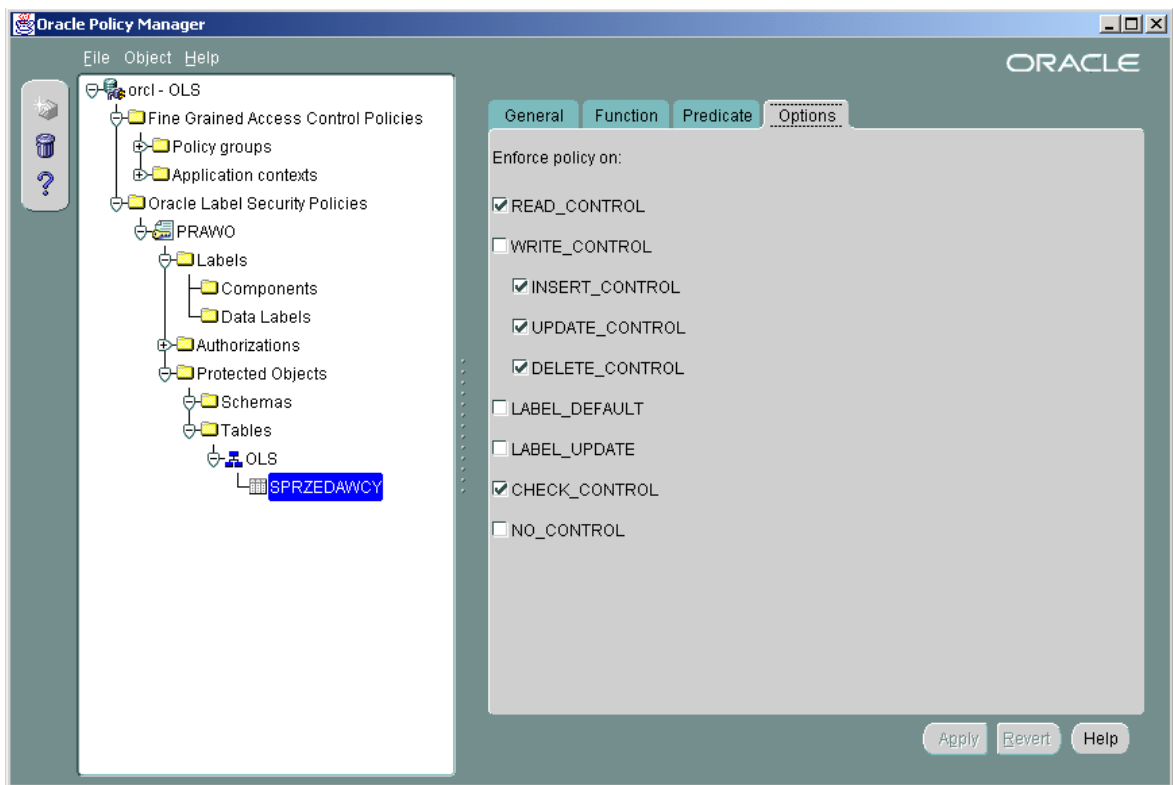
```

BEGIN
  SA_POLICY_ADMIN.REMOVE_TABLE_POLICY('prawo','OLS','sprzedawcy');
  SA_POLICY_ADMIN.APPLY_TABLE_POLICY (

```

```
policy_name => 'prawo',  
schema_name => 'OLS',  
table_name => 'sprzedawcy',  
table_options => 'READ_CONTROL,WRITE_CONTROL,CHECK_CONTROL',  
label_function =>  
'ols.get_sprzedawca_label(:new.rodzaj_klienta,:new.region,:new.kredyt)',  
predicate => NULL);  
END;  
/
```





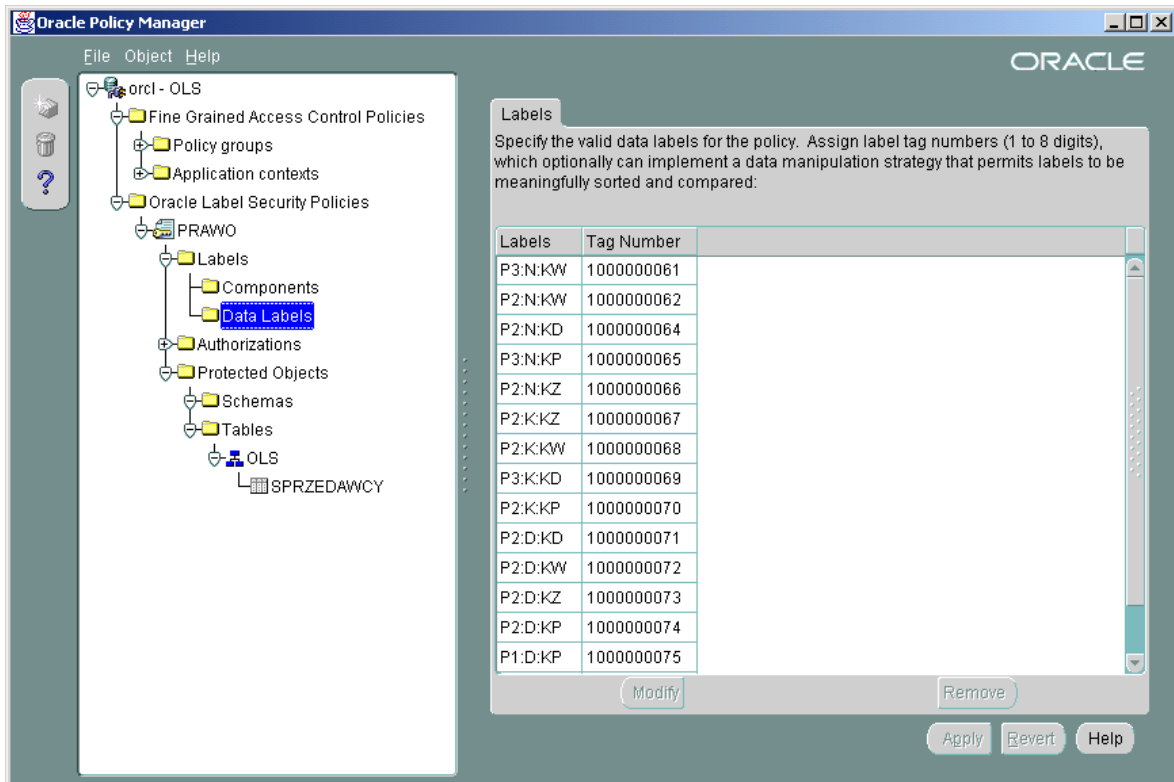
```
UPDATE sprzedawcy
SET id = id;
```

```
COMMIT;
```

The screenshot shows the Oracle Table Editor for the 'SPRZEDAWCY' table. The table contains 16 rows of data. The columns are: ID, RODZAJ_KLIENTA, IMIE, NAZWISKO, REGION, KREDYT, and ETYKIETA. The data is as follows:

ID	RODZAJ_KLIENTA	IMIE	NAZWISKO	REGION	KREDYT	ETYKIETA
1	srebrny	Pawel	Bik	WSCHOD	11000	1000000061
2	srebrny	Jacek	Gigola	WSCHOD	2000	1000000062
3	srebrny	Anna	Bajor	ZACHOD	500	1000000066
4	srebrny	Pawel	Bialy	POLUDNIE	1000	1000000064
5	srebrny	Robert	Uprzejmy	POLNOC	20000	1000000065
6	zloty	Alicja	Lopez	ZACHOD	500	1000000067
7	zloty	Katarzyna	Broszka	WSCHOD	1000	1000000068
8	zloty	Maria	Drop	ZACHOD	1000	1000000067
9	zloty	Dani	Minogue	POLUDNIE	20000	1000000069
10	zloty	Anna	Jopek	POLNOC	500	1000000070
11	platynowy	Adam	Ec	POLUDNIE	500	1000000071
12	platynowy	Anna	Klucha	WSCHOD	2000	1000000072
13	platynowy	Ewa	Prasna	ZACHOD	10000	1000000073
14	platynowy	Dariusz	Bobik	POLNOC	2000	1000000074
15	platynowy	Jan	Wstretny	POLNOC	100	1000000075
50	diamentowy	Iwan	Grozny	KRAJ	100000	1000000076

The status bar at the bottom indicates: Execute time (s): 0.05, Rows returned: 16. Buttons for 'Apply', 'Revert', 'Show SQL', 'Close', and 'Help' are visible.



12. Utworzenie użytkownika służącego do testowania dostępu do danych w przygotowanym modelu

```
CONNECT sys/sys as sysdba
```

```
CREATE USER a IDENTIFIED BY a;
```

```
GRANT CONNECT TO a;
```

```
CONNECT ols/ols
```

```
exec SA_USER_ADMIN.SET_USER_LABELS('prawo','a','P3:P,D,K,N:K');
```

```
connect a/a
```

```
select to_char(id) || '-' || label_to_char(etykieta) from ols.sprzedawcy;
```

The screenshot shows the Oracle Policy Manager interface. On the left, a tree view displays the hierarchy: orcl - OLS > Oracle Label Security Policies > PRAWO > Labels > Users > OLS. The main panel is titled 'Levels' and contains a 'Name' field with the value 'A' and a 'Browse...' button. Below this, it says 'Assign levels to the user by picking the short form:'. A table lists the available levels:

Type	Short	Long	Description
Maximum	P3	POZIOM 3	User's highest level
Minimum	P1	POZIOM 1	User's lowest level
Default	P3	POZIOM 3	User's default level
Row	P3	POZIOM 3	Row level on INSERT

At the bottom of the main panel are buttons for 'Apply', 'Revert', and 'Help'.

The screenshot shows the Oracle Policy Manager interface with the 'Compartment' tab selected. The tree view on the left is identical to the previous screenshot. The main panel is titled 'Compartment' and contains the text 'Assign compartments to the user and specify attributes:'. A table lists compartments and their attributes:

Short	Long	WRITE	DEFAULT	ROW
D	DYREKTOR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
K	KIEROWNIK	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
N	PRACOWNIK	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
P	PREZES	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

At the bottom of the main panel are buttons for 'Remove', 'Apply', 'Revert', and 'Help'.

Oracle Policy Manager

File Object Help

ORACLE

Levels Compartments **Groups** Labels Privileges Auditing

Assign groups to the user and specify attributes:

Short	Long	WRITE	DEFAULT	ROW	Parent
K	KRAJ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Remove

Apply Revert Help

Oracle Policy Manager tree structure:

- orcl - OLS
 - Fine Grained Access Control Policies
 - Policy groups
 - Application contexts
 - Oracle Label Security Policies
 - PRAWO
 - Labels
 - Components
 - Data Labels
 - Authorizations
 - Program Units
 - Users
 - OLS
 - Protected Objects
 - Schemas
 - Tables
 - OLS
 - SPRZEDAWCY