CSC12001

Data Security in Information Systems

C03 - Access Control - OLS (Oracle Label Security)

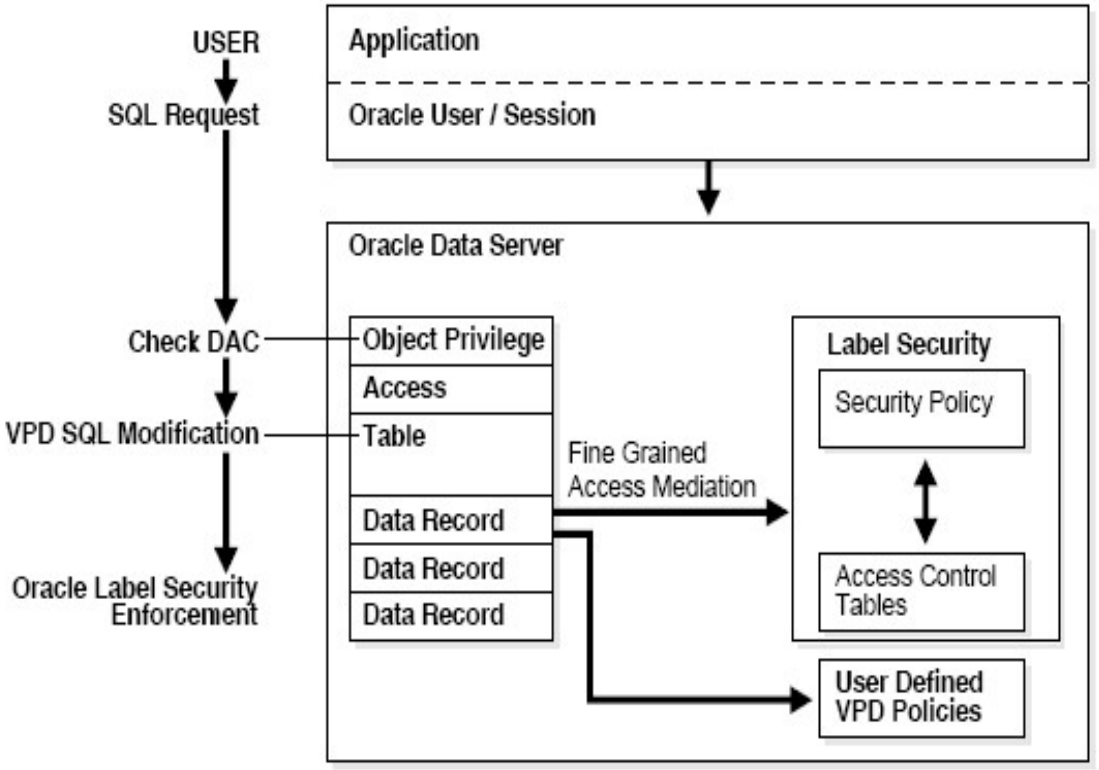
Dr. Phạm Thị Bạch Huệ
MSc. Lương Vĩ Minh

Information System Department – Faculty of Information Technology
University of Science, VNU-HCM

Introduction

- OLS was based on MAC (Mandatory Access Control):
  - Attached security labels to subjects (security clearance) and to objects (security classification)
  - Two principles: *no read-up + no write down*
  - Granting access to the data on the basis of users' clearance level and the sensitivity level of the data
  - Users have no control of security labels, but information flow is restricted to certain can-flow paths
  - Users cannot clearly know or indicate who will have what rights on the data

OLS Architecture



1. A user in a database session sends a SQL request to query a table.
2. Oracle Database checks the user's data access control (DAC) privileges for performing a SELECT statement on the table.
3. If the user does have the appropriate privileges, then Oracle Database checks if there are any Oracle Virtual Private Database (VPD) policies attached to the table.
4. Oracle Database then checks if there are any Oracle Label Security policies that are assigned to the table.
5. Oracle Label Security then compares the labels that are assigned to individual rows with the users' label authorizations, allowing or denying access.

- The session label is based on label authorizations that are assigned to the user.

Components of OLS

❑ Labels

Labels for data and users, along with authorizations for users and program units, govern access to specified protected objects. Labels are composed of the following:

- **Levels.** Levels indicate the type of sensitivity that you want to assign to the row,

For example: 1. SENSITIVE < HIGHLY SENSITIVE.
2. confidential < sensitive < highly_sensitive

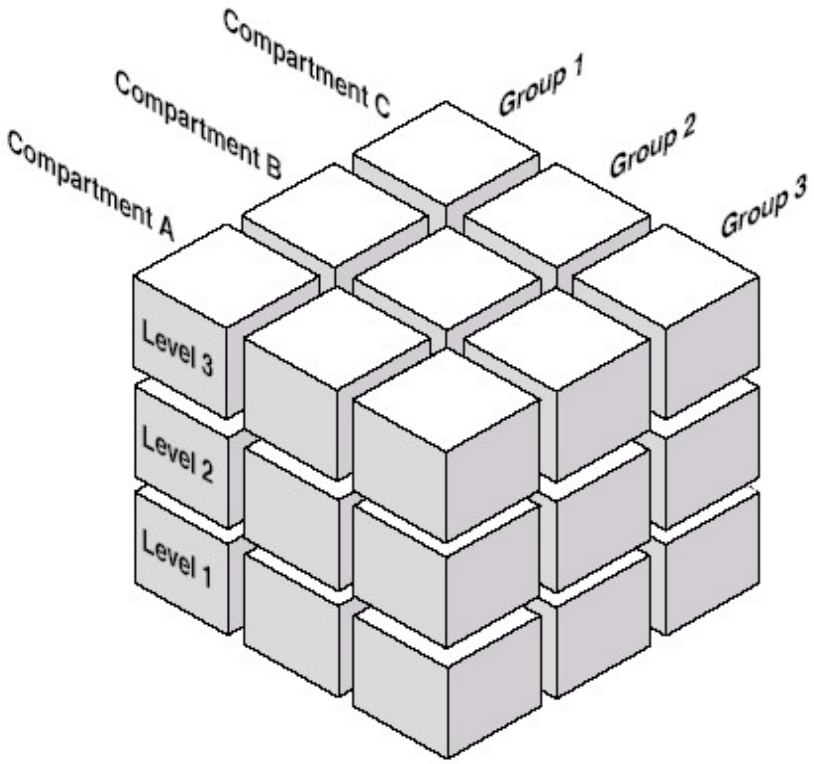
- **Compartments.** (Optional) Data can have the same level (Public, Confidential and Secret), but can belong to different projects inside a company, for example ACME Merger and IT Security.

Compartments represent the projects (in this example), or the field (FINANCIAL, STRATEGIC, NUCLEAR) that help define more precise access controls.

- **Groups.** (Optional) Groups identify organizations owning or accessing the data.

Example: UK, US, Asia, Europe.

Data Categorization



Level

- A *level* is a ranking that denotes the sensitivity of the information it labels.
- The more sensitive the information, the higher its level. The less sensitive the information, the lower its level.
- **Every label must include one level.** Oracle Label Security permits defining up to 10,000 levels in a policy → level ∈ [0, 9999].
- For each level, the administrator defines **a numeric form, a long character form, and the required short character form.**

Level (cont)

- **Numeric form**, also called **"tag"**: Administrators should avoid using sequential numbers for the numeric form of levels. A good strategy is to use even increments (such as 50 or 100) between levels. You can then insert additional levels between two preexisting levels, at a later date.
- **Long form:** The long form of the level name can contain up to 80 characters.
- **Short form:** The short form can contain up to 30 characters.

Numeric Form	Long Form	Short Form
40	*HIGHLY_SENSITIVE*	HS
30	*SENSITIVE*	S
20	*CONFIDENTIAL*	C
10	*PUBLIC*	P

- Only the short form of the name is displayed upon retrieval.

Compartment

- Compartments are optional. A label can contain zero or more compartments. OLS permits defining up to 10,000 compartments.
- Compartments identify areas that describe the sensitivity of the labeled data, providing a finer level of granularity within a level.
- Ex: FINANCIAL, CHEMICAL, OPERATIONAL

Compartment (cont)

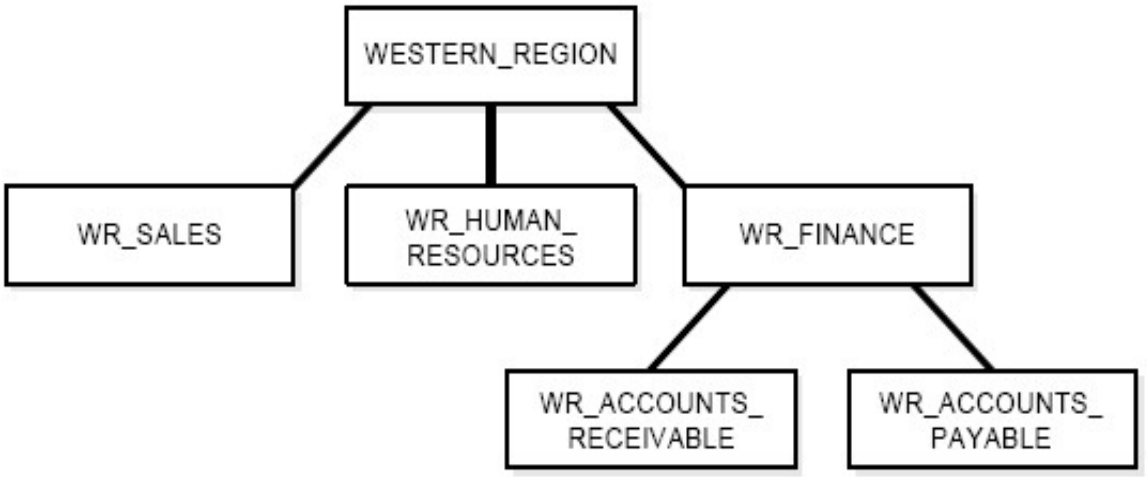
- Compartments associate the data with one or more security areas.
  - Numeric form:
    - The numeric form can range from 0 to 9999.
    - It is unrelated to the numbers used for the levels.
    - The numeric form of the compartment does not indicate greater or less sensitivity.
    - It controls the display order of the short form compartment name in the label character string.
    - For example: S:OP,CHEM,FINCL
      meaning SENSITIVE: OPERATIONAL, CHEMICAL, FINANCIAL
      The display order follows the order of the numbers assigned to the compartments: 45 < 65 < 85.
  - Long form: The long form of the compartment name scan have up to 80 characters.
  - Short form: The short form can contain up to 30 characters

Group

- Groups identify organizations owning or accessing the data.
- Ex: EASTERN_REGION, WESTERN_REGION, WR_SALES.
- All data pertaining to a certain department can have that department's group in the label.
- Groups are useful for the controlled dissemination of data and for timely reaction to organizational change. When a company reorganizes, data access can change right along with the reorganization.

Group

- Groups are hierarchical.
- You can label data based upon your organizational infrastructure.
- A group can thus be associated with a parent group.
- For example, you can define a set of groups corresponding to the following organizational hierarchy:



Numeric Form	Long Form	Short Form	Parent Group
1000	WESTERN_REGION	WR	
1100	WR_SALES	WR_SAL	WR
1200	WR_HUMAN_RESOURCES	WR_HR	WR
1300	WR_FINANCE	WR_FIN	WR
1310	WR_ACCOUNTS_PAYABLE	WR_AP	WR_FIN
1320	WR_ACCOUNTS_RECEIVABLE	WR_AR	WR_FIN

Group

- Groups are optional; a label can contain zero or more groups.
- OLS permits defining up to 10,000 groups.
- All labels need not have groups.
- When you analyze the sensitivity of data, you may find that some groups are only used at specific levels.
- For example, you can specify HIGHLY_SENSITIVE and CONFIDENTIAL labels with no groups, and a SENSITIVE label that does contain groups.

Group

- Numeric form: The numeric form of the group can range from 0 to 9999, and it must be unique for each policy.
  The numeric form does not indicate any kind of ranking. It does not indicate a parent-child relationship, or greater or less sensitivity.
- It only controls the display order of the short form group name in the label character string.
  For example, S:CHEM:WR,WR_HR
  (a label is created that has the level SENSITIVE, the compartment CHEMICAL, and the groups WESTERN_REGION and WR_HUMAN_RESOURCES with the corresponding short forms).
  WR is displayed before WR_HR because 1000 comes before 1200.
- Long form: The long form of the group name can contain up to 80 characters.
- Short form: The short form can contain up to 30 characters.

Group

- Groups are optional; a label can contain zero or more groups.
- Oracle Label Security permits defining up to 10,000 groups.
  All labels need not have groups. When you analyze the sensitivity of data, you may
  find that some groups are only used at specific levels.
- For example:
  - You can specify HIGHLY_SENSITIVE and CONFIDENTIAL labels with no groups,
  - And a SENSITIVE label that does contain groups.

Label Syntax

LEVEL:COMPARTMENT1,…, COMPARTMENTn:GROUP1, …, GROUPn

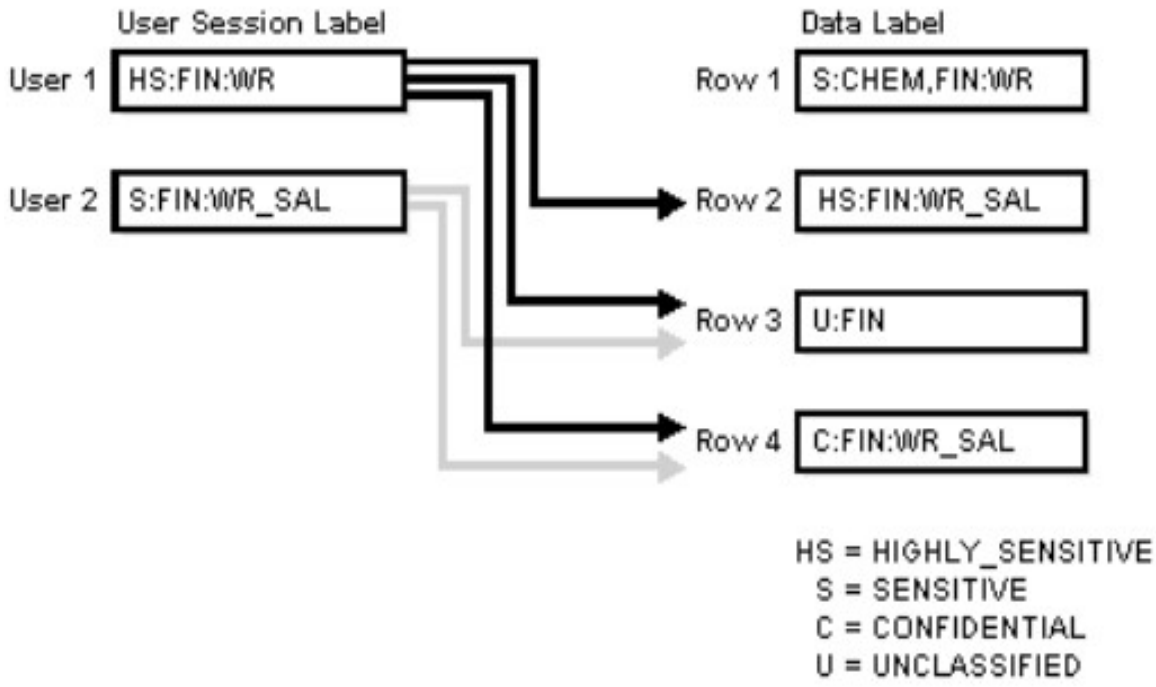
- A label must have a level.
- The text string specifying the label can have a maximum of 4,000 characters, including alphanumeric characters, spaces, and underscores. The labels are case-insensitive.
- **Example:**
  - **SENSITIVE:FINANCIAL,CHEMICAL:EASTERN_REGION,WESTERN_REGION**
  - **CONFIDENTIAL:FINANCIAL:VP_GRP**
  - **SENSITIVE**
  - **HIGHLY_SENSITIVE:FINANCIAL**
  - **SENSITIVE:WESTERN_REGION**

READ Algorithm

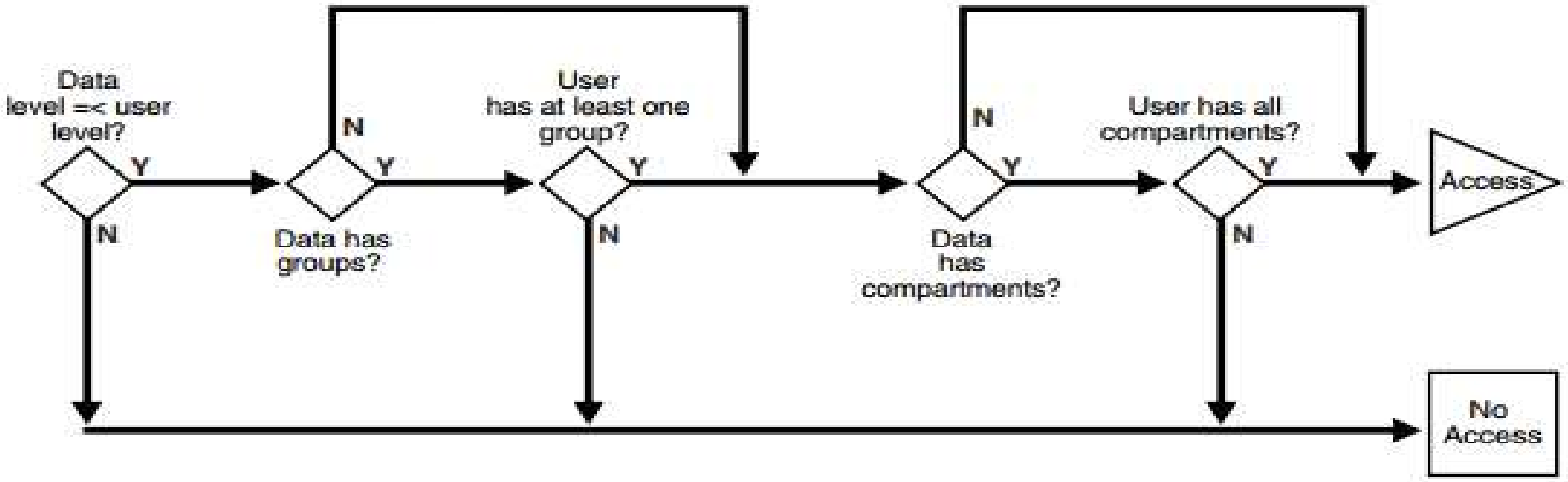
- The READ_CONTROL enforcement determines the ability to read data in a row.
- The following rules are used, in the sequence listed, to determine a user's read access to a row of data:
  1. The user's level must be *greater than or equal to* the level of the data.
  2. The user's label must include *at least one of the groups* that belong to the data (or the parent group of one such subgroup).
  3. The user's label must include *all the compartments* that belong to the data.
  If the user's label passes these tests, then it is said to dominate the row's label

READ Algorithm

- At any time, the user can read all data equal to or less than the current session level. No privileges (other than FULL) allow the user to write below the minimum authorized level.



Label Evaluation Process for Read Access



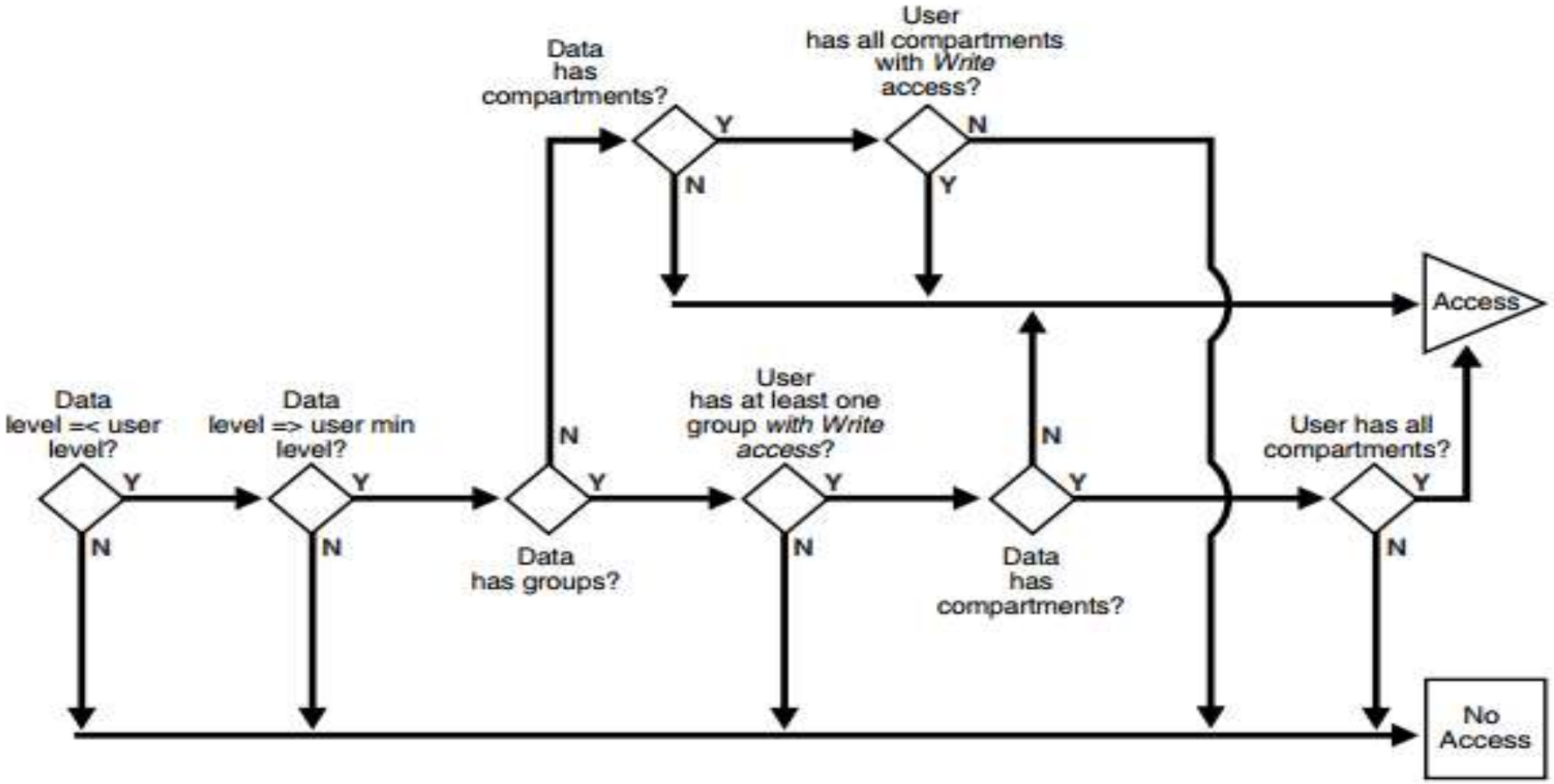
- OLS policies allow user sessions to read rows at their label and below, which is called *reading down*.
- Sessions cannot read rows at labels that they do not dominate.

WRITE Algorithm

- WRITE_CONTROL enforcement determines the ability to insert, update, or delete data in a row
- To determine whether a user can write a particular row of data, OLS evaluates the following rules, in the order given:

  1. The level in the data label must be greater than or equal to the user's minimum level and less than or equal to the user's session level.
  2. When groups are present, the user's label must include *at least one of the groups with write access* that appear in the data label (or the parent of one such subgroup). In addition, the user's label must include *all the compartments* in the data label.
  3. When no groups are present, the user's label must have write access on *all of the compartments* in the data label.
- If the label has *no* groups, then the user must have write access on all the compartments in the label in order to write the data.
- If the label *does* have groups and the user has write access to one of the groups, she only needs read access to the compartments in order to write the data.

Label Evaluation Process for Write Access



Notes

- The label evaluation process proceeds from levels to groups to compartments.
- Note that the user cannot write any data below the authorized minimum level, nor above the current session level.
- The user can always read below the minimum level.

Notes

- Write access is enforced on INSERT, UPDATE and DELETE operations upon the data in the row.
- Each user may have an associated minimum level below which the user cannot write.
  - The user cannot update or delete any rows labeled with levels below the minimum,
  - The user cannot insert a row with a row label containing a level less than the minimum.

- User không thể ghi dữ liệu có level < minimum level của user
- User không thể ghi dữ liệu có level > current session level của user.
- User chỉ có thể đọc dữ liệu có level < minimum level của user.

Implementing Label Security

There are five steps necessary to implement OLS:

1. *Create the OLS policy.*
2. *Define the OLS label components.*
3. *Create the actual OLS labels you wish to use.*
4. *Apply the OLS security policy (labels) to your table(s) or schemas.*
5. *Assign the label authorizations to be used by the users or applications.*

- SCOTT schema: data tables reside in this schema.

```
CREATE TABLE announcements (MESSAGE VARCHAR2(4000));
```

.

- SEC_MGR schema: security policies reside in this schema.

Creating the policy

- A policy is the container for everything:
  - The labels,
  - user authorizations,
  - and the protected objects

- You have to define the name of the column that will be used to hold your labels.
  Ex: “ROWLABEL”
- The choice for your column is important because the column name will be appended to the tables on which you want to enforce your OLS policies.
- The label column name has to be unique among all the OLS policies in your database.

Step 1: Creating OLS policy

- Invoking SA_SYSDBA.CREATE_POLICY procedure.
- Privileges to execute this procedure have been granted to the default OLS administrator known as LBACSYS.

```
lbacsys> BEGIN
 sa_sysdba.create_policy
(policy_name => 'ESBD',
column_name => 'rowlabel');
END;
```

(ESBD: Effective Security By Design)

Step 1: Creating the OLS policy

- When a policy is created, Oracle automatically creates an administrator database role for the policy. The role name is the policy's name appended with "_DBA".
- Example: For the ESBD policy created above, the role name is ESBD_DBA. This role and the privileges granted to it will be used for this example.

- When you grant the ESBD_DBA role to the SEC_MGR schema, you're bestowing administration privileges for the ESBD policy to the SEC_MGR user:

```
lbacsys> -- Privs and authorization to administer the ESBD
policy
lbacsys> GRANT esbd_dba TO sec_mgr;
```

Notes

- OLS allows you to create multiple policies and apply the labels to only selected users and objects.
- When you create the policy, you have to define the name of the column that will be used to hold your labels.
- Suppose that the name of the label column is “ROWLABEL”. The column name “ROWLABEL” will be appended to the tables on which you want to enforce your OLS policies.
- The label column name has to be unique among all the OLS policies in your database.

Least Privileges for OLS Administrators

- The SEC_MGR will perform all the OLS administration duties. The following privileges are therefore required:
- Privs to create components that make up valid labels

```
lbacsys> GRANT EXECUTE ON sa_components TO sec_mgr;
```

- Privileges to create the valid labels

```
lbacsys> GRANT EXECUTE ON sa_label_admin TO sec_mgr;
```

- Privileges to assign authorization labels to users

```
lbacsys> GRANT EXECUTE ON sa_user_admin TO sec_mgr;
```

- Privileges to convert a character string to its numeric label representation

```
lbacsys> GRANT EXECUTE ON char_to_label TO sec_mgr;
```

Label components

- The label components are the names and the relationships of the different classifications the policy will contain.
- The policy administrator requires two things to create components: execute privileges on the SA_COMPONENTS package and the policy's database role.
- A label is composed of three components: at least one level, zero or more compartments, and zero or more groups.

Step 2.1: Create the label components

- Creating levels, suppose that there are three levels:

Number	Long name	Short name
9000	Executive Staff	EXEC
8000	Manager	MGR
7000	Employee	EMP

```
sa_components.create_level
(policy_name => 'ESBD',
long_name => 'Executive Staff',
short_name => 'EXEC',
level_num => 9000);
```

Step 3.1 Creating the label

- Case 1: Label with only level component.

- The SA_LABEL_ADMIN package allows you to create the labels. The execute privilege was granted directly to the SEC_MGR.

LABEL_TAG parameter

- The labels, like the level component, contain a number as represented by the LABEL_TAG parameter.
- The label tag does not imply the label's security.
- The label tag is the actual number that is stored in the security column when the policy is eventually applied to the database table(s).
- Label tag number has to be unique for all labels in all policies in the database.

Step 3.1: Creating the label (Cont)

	Label tag	Label value
Labels consist of only level	1	EXEC
	2	MGR
	3	EMP

Example:

```
sa_label_admin.create_label
(policy_name => 'ESBD',
label_tag => 1,
label_value => 'EXEC');
```

Data records in ANNOUNCEMENTS table

Announcements
This message is only for the Executive Staff.
All Managers: employee compensation announcement…
This message is to notify all employees…

Step 4.1: Applying the policy

- Applying the OLS policy (labels) to the table by executing the APPLY_TABLE_POLICY procedure of the SA_POLICY_ADMIN package.

Purpose	Table-Level Function	Schema-Level Function
Apply policy	APPLY_TABLE_POLICY	APPLY_SCHEMA_POLICY
Alter policy	Not applicable	ALTER_SCHEMA_POLICY
Disable policy	DISABLE_TABLE_POLICY	DISABLE_SCHEMA_POLICY
Re-enable policy	ENABLE_TABLE_POLICY	ENABLE_SCHEMA_POLICY
Remove policy	REMOVE_TABLE_POLICY	REMOVE_SCHEMA_POLICY

Step 4.1: Applying the policy

- Ta có thể gán chính sách cho:
  - Table: chính sách chỉ bảo vệ table
  - Schema: tất cả các table của schema đều được bảo vệ
  - Nếu gán chính sách cho schema và sau đó lại gán chính sách cho một table thuộc schema đó thì các tùy chọn, thao tác ở cấp độ table sẽ ưu tiên hơn so với các tùy chọn thao tác ở cấp độ schema.
-

Purpose	Table-Level Function	Schema-Level Function
Apply policy	APPLY_TABLE_POLICY	APPLY_SCHEMA_POLICY
Alter policy	Not applicable	ALTER_SCHEMA_POLICY
Disable policy	DISABLE_TABLE_POLICY	DISABLE_SCHEMA_POLICY
Re-enable policy	ENABLE_TABLE_POLICY	ENABLE_SCHEMA_POLICY
Remove policy	REMOVE_TABLE_POLICY	REMOVE_SCHEMA_POLICY

Step 4.1: Applying the policy

```
sa_policy_admin.apply_table_policy
(policy_name => 'ESBD',
schema_name => 'SCOTT',
table_name => 'ANNOUNCEMENTS',
table_options => 'NO_CONTROL');
```

- Applying a policy to the table alters the table and adds the label column.
- You can see the effect of the APPLY_TABLE_POLICY procedure by looking at the table's structure.

```
scott> DESCRIBE announcements
Name                                      Type
----------------------------------------- -------- --------------
MESSAGE                                   VARCHAR2(4000)
ROWLABEL                                  NUMBER(10)
```

Step 4.1: Applying the policy

- To begin, choose the 'NO_CONTROL' option indicating that you don't want OLS to enforce any security.
- Until the label column values are populated, you'll not be able to access any of the data. That is, OLS returns no records when the label values are undefined or are null.

```
sec_mgr> BEGIN
 sa_policy_admin.apply_table_policy
 (policy_name => 'ESBD',
 schema_name => 'SCOTT',
 table_name => 'ANNOUNCEMENTS',
 table_options => 'NO_CONTROL');
 END;
```

Step 4.1: Applying the policy

- SEC_MGR will set the values for records by one of the following ways:
  - C1: Assigns manually by using INSERT or UPDATE.
  - C2: Use the option LABEL_DEFAULT.
  - C3: Use the function to assign the labels for records automatically. The function will be executed when there are INSERT or UPDATE command on the data:

- We use C1 from now on.

Step 4.1: Applying the policy

- The SEC_MGR can now update the OLS labels.
- The SEC_MGR doesn't have the privileges to query or update the ANNOUNCEMENT table. So, SCOTT has to grant the DAC object-level privileges on the table:

```
scott> GRANT SELECT, INSERT, UPDATE
2 ON announcements TO sec_mgr;
Grant succeeded.
```

- SEC_MGR do the following updates:

```
-- Set all records to lowest level
UPDATE scott.announcements
SET ROWLABEL = char_to_label ('ESBD', 'EMP');
-- Increase level for manager's records
UPDATE scott.announcements
SET ROWLABEL = char_to_label ('ESBD', 'MGR')
WHERE UPPER (MESSAGE) LIKE '%MANAGE%';
-- Increase level for manager's records
UPDATE scott.announcements
SET ROWLABEL = char_to_label ('ESBD', 'EXEC')
WHERE UPPER (MESSAGE) LIKE '%EXECUTIVE%';
```

Data records to be labeled

Announcements	ROWLABEL
This message is only for the Executive Staff.	EXEC
All Managers: employee compensation announcement…	MGR
This message is to notify all employees…	EMP

Step 5.1: Create the user authorizations

- 3 authorizations will be created:
  - “ALL_EMPLOYEES”: representing general employees.
  - “ALL_MANAGERS”: for managers.
  - “ALL_EXECS”: for executives.

```
sa_user_admin.set_user_labels
(policy_name => 'ESBD',
user_name => 'ALL_EMPLOYEES',
max_read_label => 'EMP');

sa_user_admin.set_user_labels
(policy_name => 'ESBD',
user_name => 'ALL_MANAGERS',
max_read_label => 'MGR');

sa_user_admin.set_user_labels
(policy_name => 'ESBD',
user_name => 'ALL_EXECS',
max_read_label => 'EXEC');
```

Testing the labels

- To change the policy enforcement options, you have to first remove the policy with NO_CONTROL enforcement and then re-add it with the READ_CONTROL enforcement option, which will restrict all select operations on the table:

sec_mgr:

```
sa_policy_admin.remove_table_policy
(policy_name => 'ESBD',
schema_name => 'SCOTT',
table_name => 'ANNOUNCEMENTS');
```

```
sa_policy_admin.apply_table_policy
(policy_name => 'ESBD',
schema_name => 'SCOTT',
table_name => 'ANNOUNCEMENTS',
table_options => 'READ_CONTROL');
```

Specific authorizations of OLS

- A user can be granted the pre-defined authorizations of OLS.
- Sec_mgr kích hoạt quyền PROFILE_ACCESS để có thể chuyển đổi profile.
- Some privileges allowed the authorized user to bypass the specific label security enforcements:
  - **PROFILE ACCESS** Allows the user to switch their security profile
  - **READ** Allows the user to select any data. This is valuable for inspecting labels and performing exports of data.
  - **WRITE** Allows the user to override the OLS protections for each of the label components.
  - **FULL** This is the shortcut for granting both read and write privileges.

  The privileges are unique to OLS and only can be enabled by invoking the SA_USER_ADMIN.SET_USER_PRIVS

- The profile access privilege allows a user to set their security authorizations to that of another (user's) profile:

```
sa_user_admin.set_user_privs
(policy_name => 'ESBD',
user_name => 'SEC_MGR',
PRIVILEGES => 'PROFILE_ACCESS');
```

- The SEC_MGR can now set the OLS security profile to be any one of the three authorization "users" just defined.
  Ex: như ALL_EMPLOYEES, hoặc ALL_MANAGERS, hoặc ALL_EXECS

- sec_mgr resets his profile to ALL_EMPLOYEES, relogging:

```
sa_session.set_access_profile ('ESBD', 'ALL_EMPLOYEES')
SELECT MESSAGE
FROM SCOTT.ANNOUNCEMENTS;
```

→ Result:

```
This message is to notify all employees…
```

- sec_mgr resets his profile to ALL_MANAGERS

```
sa_session.set_access_profile ('ESBD', 'ALL_MANAGERS')
SELECT MESSAGE
FROM SCOTT.ANNOUNCEMENTS;
```

→ Results:

```
This message is to notify all employees…
All Managers: employee compensation announcement…
```

- sec_mgr resets his profile to ALL_EXECS

```
sa_session.set_access_profile ('ESBD', 'ALL_EXECS')
SELECT MESSAGE
FROM SCOTT.ANNOUNCEMENTS;
```

→ Result:

```
This message is to notify all employees…
All Managers: employee compensation announcement…
This message is only for the Executive Staff.
```

- To get the label of the current user:

```
COL "Read Label" format a25
SELECT sa_session.read_label('ESBD') "Read Label"
From DUAL;
```

→ Result:

```
Read Label
---------------------------
EXEC
```

- We consider the case that labels consist of 2 components: level and compartment.

- Supose that we wish to post messages to a subgroup of the employees, managers, or executives.
- To do this, three categories or compartments, for example, can be added. There will be:
  - One category for sales employees,
  - One for developers,
  - Another for the remaining employees who generally support the internal systems for support and development.

Step 2.2 Create the compartments

- There are subgroups in each group, except Executive.
  - Employees: products sales, products development, internal support.
  - Managers: sales managers, development managers.
  - Executive.

- Your will create 3 compartments:

Numeric form	Long form	Short form
1000	Product Sales	SALES
100	Product Development	DEV
10	Internal Support	IS

Example

```
sa_components.create_compartment
(policy_name => 'ESBD',
long_name => 'Product Sales',
short_name => 'SALES',
level_num => 1000);
```

The policies

- Employees with compartment authorizations will see all the data within their compartment and the data that has no compartments.
- Managers can see:
  - The messages for managers within their compartment. Development managers can’t see any sales data regardless of the level of that data.
  - The messages for all the managers.
  - The messages for employees within the same compartment.
  - The messages that all the employees can see.
- Modify the label for executives for reading all the messages.

Step 3.2 Create the labels

- We create the following labels:

	Label tag	Label value
Labels with level and compartment(s)	10	EXEC:SALES, DEV, IS
	20	MGR:SALES
	25	MGR:DEV
	30	EMP:SALES
	35	EMP:DEV
	39	EMP:IS

Step 3.2: Create the labels

- Example:

```
sa_label_admin.create_label
(policy_name => 'ESBD',
label_tag => 10,
label_value => 'EXEC:SALES,DEV,IS');
```

Authorizations for Compartments

- Create the authorizations that will allow access to the new compartment labels.
  - **For the executives, modify the current authorization to add the new compartments** by executing the ADD_COMPARTMENTS procedure:

```
sec_mgr> BEGIN
sa_user_admin.add_compartments
(policy_name => 'ESBD',
user_name => 'ALL_EXECS',
comps => 'SALES,DEV,IS');
END;
```

Step 4.2 Authorizations for compartments

- Existing authorizations:
  - "ALL_EMPLOYEES": now can read the messages that all employees can read.
  - "ALL_MANAGERS": now can read the messages that all managers can read .
  - "ALL_EXECS": had been modified, can read all the messages.
- Create new authorizations:

User categories	Authorizations	Max_read_label	Privileges
Executive Staff	ALL_EXECS (modified)	EXEC:SALES,DEV,IS	Can read all the messages
Manager	SALES_MANAGERS	MGR:SALES	Managers can see data for all mployees (no compartments), for all managers, and only the data within their compartment(s).
	DEV_MANAGERS	MGR:DEV	As above
Employees	SALES_EMPLOYEES	EMP:SALES	Can see all the data within their compartment and the data that has no compartments.
	DEV_EMPLOYEES	EMP:DEV	As above
	INTERNAL_EMPLOYEES	EMP:IS	As above

Adding more messages

Messages	ROWLABEL	Notes
This message is only for the Executive Staff.	EXEC	Only for EXEC staff
All Managers: employee compensation announcement…	MGR	For all managers
This message is to notify all employees…	EMP	For all the employees
New updates to quotas have been assigned (sales managers)	MGR:SALES	Only for sales managers
New product release date meeting scheduled (dev. managers)	MGR:DEV	Only for dev. managers
Quota club trip destined for Hawaii (sales emp.)	EMP:SALES	For sales emp.
Source control software updates distributed next week (dev. emp)	EMP:DEV	For dev. emp
Firewall attacks increasing (i.s. emp.)	EMP:IS	For i.s. emp.

Testing

ALL_EMPLOYEES

Max_read_label : EMP

Messages	ROWLABEL	Notes
This message is only for the Executive Staff.	EXEC	Only for EXEC staff
All Managers: employee compensation announcement…	MGR	For all managers
This message is to notify all employees…	EMP	For all the employees
New updates to quotas have been assigned (sales managers)	MGR:SALES	Only for sales managers
New product release date meeting scheduled (dev. managers)	MGR:DEV	Only for dev. managers
Quota club trip destined for Hawaii (sales emp.)	EMP:SALES	For sales emp.
Source control software updates distributed next week (dev. emp)	EMP:DEV	For dev. emp
Firewall attacks increasing (i.s. emp.)	EMP:IS	For i.s. emp.

Testing

ALL_MANAGERS

Max_read_label : MGR

Messages	ROWLABEL	Notes
This message is only for the Executive Staff.	EXEC	Only for EXEC staff
All Managers: employee compensation announcement…	MGR	For all managers
This message is to notify all employees…	EMP	For all the employees
New updates to quotas have been assigned (sales managers)	MGR:SALES	Only for sales managers
New product release date meeting scheduled (dev. managers)	MGR:DEV	Only for dev. managers
Quota club trip destined for Hawaii (sales emp.)	EMP:SALES	For sales emp.
Source control software updates distributed next week (dev. emp)	EMP:DEV	For dev. emp
Firewall attacks increasing (i.s. emp.)	EMP:IS	For i.s. emp.

Testing

ALL_EXECS

Max_read_label : EXEC:SALES,DEV,IS

Messages	ROWLABEL	Notes
This message is only for the Executive Staff.	EXEC	Only for EXEC staff
All Managers: employee compensation announcement…	MGR	For all managers
This message is to notify all employees…	EMP	For all the employees
New updates to quotas have been assigned (sales managers)	MGR:SALES	Only for sales managers
New product release date meeting scheduled (dev. managers)	MGR:DEV	Only for dev. managers
Quota club trip destined for Hawaii (sales emp.)	EMP:SALES	For sales emp.
Source control software updates distributed next week (dev. emp)	EMP:DEV	For dev. emp
Firewall attacks increasing (i.s. emp.)	EMP:IS	For i.s. emp.

Testing

SALES_MANAGERS

Max_read_label : MGR:SALES

Messages	ROWLABEL	Notes
This message is only for the Executive Staff.	EXEC	Only for EXEC staff
All Managers: employee compensation announcement…	MGR	For all managers
This message is to notify all employees…	EMP	For all the employees
New updates to quotas have been assigned (sales managers)	MGR:SALES	Only for sales managers
New product release date meeting scheduled (dev. managers)	MGR:DEV	Only for dev. managers
Quota club trip destined for Hawaii (sales emp.)	EMP:SALES	For sales emp.
Source control software updates distributed next week (dev. emp)	EMP:DEV	For dev. emp
Firewall attacks increasing (i.s. emp.)	EMP:IS	For i.s. emp.

Testing

DEV_MANAGERS

Max_read_label : MGR:DEV

Messages	ROWLABEL	Notes
This message is only for the Executive Staff.	EXEC	Only for EXEC staff
All Managers: employee compensation announcement…	MGR	For all managers
This message is to notify all employees…	EMP	For all the employees
New updates to quotas have been assigned (sales managers)	MGR:SALES	Only for sales managers
New product release date meeting scheduled (dev. managers)	MGR:DEV	Only for dev. managers
Quota club trip destined for Hawaii (sales emp.)	EMP:SALES	For sales emp.
Source control software updates distributed next week (dev. emp)	EMP:DEV	For dev. emp
Firewall attacks increasing (i.s. emp.)	EMP:IS	For i.s. emp.

Testing

SALES_EMLOYEES

Max_read_label : EMP:SALES

Messages	ROWLABEL	Notes
This message is only for the Executive Staff.	EXEC	Only for EXEC staff
All Managers: employee compensation announcement…	MGR	For all managers
This message is to notify all employees…	EMP	For all the employees
New updates to quotas have been assigned (sales managers)	MGR:SALES	Only for sales managers
New product release date meeting scheduled (dev. managers)	MGR:DEV	Only for dev. managers
Quota club trip destined for Hawaii (sales emp.)	EMP:SALES	For sales emp.
Source control software updates distributed next week (dev. emp)	EMP:DEV	For dev. emp
Firewall attacks increasing (i.s. emp.)	EMP:IS	For i.s. emp.

Testing

DEV_EMPLOYEES

Max_read_label : EMP:DEV

Messages	ROWLABEL	Notes
This message is only for the Executive Staff.	EXEC	Only for EXEC staff
All Managers: employee compensation announcement…	MGR	For all managers
This message is to notify all employees…	EMP	For all the employees
New updates to quotas have been assigned (sales managers)	MGR:SALES	Only for sales managers
New product release date meeting scheduled (dev. managers)	MGR:DEV	Only for dev. managers
Quota club trip destined for Hawaii (sales emp.)	EMP:SALES	For sales emp.
Source control software updates distributed next week (dev. emp)	EMP:DEV	For dev. emp
Firewall attacks increasing (i.s. emp.)	EMP:IS	For i.s. emp.

Testing

INTERNAL_EMPLOYEES

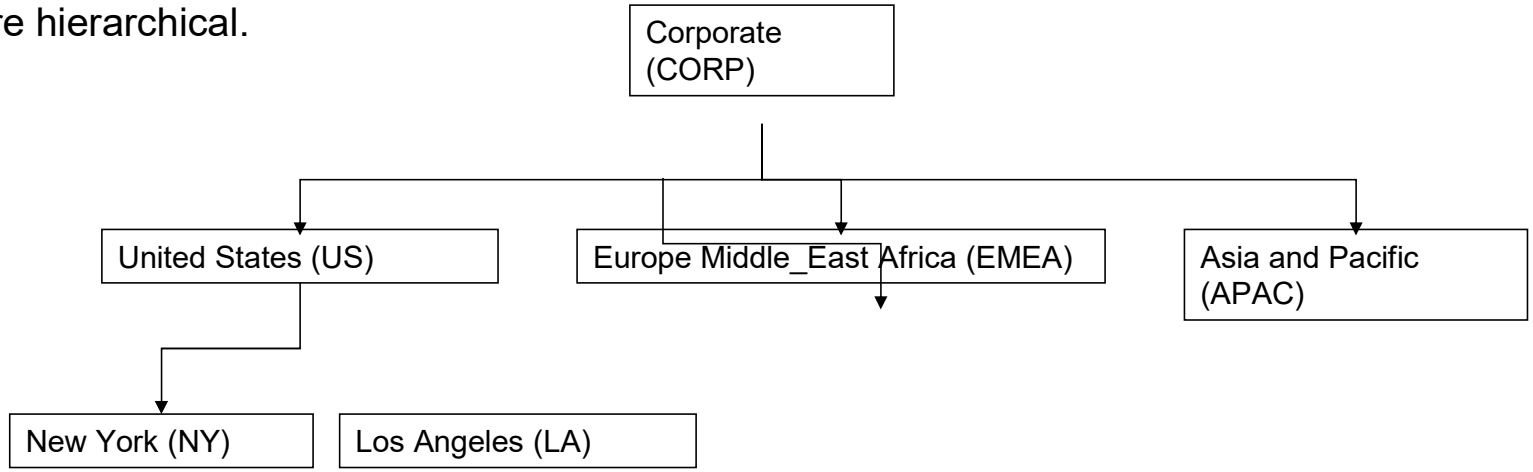
Max_read_label : EMP:IS

Messages	ROWLABEL	Notes
This message is only for the Executive Staff.	EXEC	Only for EXEC staff
All Managers: employee compensation announcement…	MGR	For all managers
This message is to notify all employees…	EMP	For all the employees
New updates to quotas have been assigned (sales managers)	MGR:SALES	Only for sales managers
New product release date meeting scheduled (dev. managers)	MGR:DEV	Only for dev. managers
Quota club trip destined for Hawaii (sales emp.)	EMP:SALES	For sales emp.
Source control software updates distributed next week (dev. emp)	EMP:DEV	For dev. emp
Firewall attacks increasing (i.s. emp.)	EMP:IS	For i.s. emp.

- The case that labels consist of 3 components: level, compartment and group.

Step 2.3: Creating groups

Groups are hierarchical.



Group num	Parent_name	Long name	Short name
1	NULL	Corporate	CORP
100	CORP	United State	US
110	US	New York	NY
120	US	Los Angeles	LA
200	CORP	Europe Middle_East Africa	EMEA
300	CORP	Asia and Pecific	APAC

Step 2.3: Creating groups

```
sa_components.CREATE_GROUP
policy_name => 'ESBD',
long_name => 'Corporate',
short_name => 'CORP',
group_num => 1,
parent_name => NULL);

sa_components.CREATE_GROUP
policy_name => 'ESBD',
long_name => 'United States',
short_name => 'US',
group_num => 100,
parent_name => 'CORP');
```

```
sa_components.CREATE_GROUP
(policy_name => 'ESBD',
long_name => 'New York',
short_name => 'NY',
group_num => 110,
parent_name => 'US');

sa_components.CREATE_GROUP
 (policy_name => 'ESBD',
 long_name => 'Los Angeles',
 short_name => 'LA',
 group_num => 120,
 parent_name => 'US');
```

Step 3.3: Creating the labels

	Labels	Label tag
Sales managers of EMEA	MGR:SALES:EMEA	300
Sales manager for al US	MGR:SALES:US	310
New York sales prepresentatives	EMP:SALES:NY	320
Los Angeles sales representatives	EMP:SALES:LA	330
US developers	EMP:DEV:US	400
APAC developers	EMP:DEV:APAC	410
Developer managers for CORP	MGR:DEV:CORP	450
Executives	EXEC:SALES, DEV, IS: CORP	

Step 4.2 Authorizations for compartments

- Existing authorizations:
  - "ALL_EMPLOYEES": now can read the messages that all employees can read.
  - "ALL_MANAGERS": now can read the messages that all managers can read .
  - "ALL_EXECS": modified by adding "CORP" group, can read all the messages.
- Create new authorizations:

User categories	Authorizations	Max_read_label	Privileges
Executive Staff	ALL_EXECS (modified)	EXEC:SALES,DEV,IS:CORP	Can read all the messages
Manager	US_SALES_MANAGERS (modified)	MGR:SALES:US	Managers can see data for all mployees (no compartments), for all managers, and only the data within their compartment(s).
	DEV_MANAGERS (modified)	MGR:DEV:CORP	As above
	EMEA_SALES_MGR	MGR:SALES:EMEA	
	NY_SALES_REP	EMP:SALES:NY	
	LA_SALES_REP	EMP:SALES:LA	
	APAC_DEVELOPER	EMP:DEV:APAC	
	US DEVELOPER	EMP:DEV:US	

Step 4.3: Assign the labels to users

- Adding groups to executives. Only need to add root group:

```
sec_mgr> BEGIN
sa_user_admin.add_groups
(policy_name => 'ESBD',
user_name => 'ALL_EXECS',
groups => 'CORP');
END;
```

- Create authorizations for US and EMEA sales managers

```
sec_mgr@KNOX10g> BEGIN
sa_user_admin.set_user_labels
(policy_name => 'ESBD',
user_name => 'US_SALES_MGR’,
   max_read_label => 'MGR:SALES:US’);
```

-
```
sa_user_admin.set_user_labels
(policy_name => 'ESBD',
user_name => 'EMEA_SALES_MGR',
max_read_label => 'MGR:SALES:EMEA');
END;
```

-

- sec_mgr> BEGIN
  sa_user_admin.set_user_labels
  (policy_name => 'ESBD',
  user_name => 'NY_SALES_REP',
  max_read_label => 'EMP:SALES:NY');
  sa_user_admin.set_user_labels
  (policy_name => 'ESBD',
  user_name => 'LA_SALES_REP',
  max_read_label => 'EMP:SALES:LA');
  END;

- You saw how data can be labeled by issuing an update statement to the table and by including the label in the insert
statement. Another interesting technique for labeling data is to use an OLS capability, which will create the label automatically.
- The option is called LABEL_DEFAULT. When enabled, OLS will use a database trigger to populate the
label column based on the user's current (write) authorization label. To do this, you have to change the policy options.

-

- Use default write session, we have to drop then re-add policy with label_default option.
  sec_mgr> BEGIN
  sa_policy_admin.remove_table_policy
   (policy_name => 'ESBD',
  schema_name => 'SCOTT',
  table_name => 'ANNOUNCEMENTS’);
-
  sa_policy_admin.apply_table_policy
  (policy_name => 'ESBD',
  schema_name => 'SCOTT',
  table_name => 'ANNOUNCEMENTS',
  table_options => '**LABEL_DEFAULT**,READ_CONTROL');
  END;

- To insert data now, you can omit the ROWLABEL column, and OLS will use the user's current write label to populate the data's label.
- The write label can be the same as the read label in this example.
- If you set the session profile (authorization) to the US sales managers and insert data, the data is automatically tagged as MGR:SALES:US.
- Insert data as a US sales manager. OLS will automatically label data based on user's write label.

```
sec_mgr > BEGIN sa_session.set_access_profile ('ESBD',
'US_SALES_MGR');
END;

PL/SQL procedure successfully completed.
```

- sec_mgr> INSERT INTO scott.announcements
  (MESSAGE)
  VALUES ('Presidential outlook for economy may affect revenue.');
  1 row created.
- sec_mgr> COMMIT ;
  Commit complete.

- Check label of inserted message
  sec_mgr> SELECT MESSAGE, label_to_char (ROWLABEL) "OLS Label"
  FROM scott.announcements
  WHERE MESSAGE LIKE 'Pres%';

MESSAGE	OLS Label
Presidential outlook for economy may affect revenue.	MGR:SALES:US

Adding data records

MESSAGE	OLS Label
This message is only for the Executive Staff.	EXEC
All Managers: employee compensation announcement...	MGR
This message is to notify all employees...	EMP
New updates to quotas have been assigned.	MGR:SALES
New product release date meeting scheduled.	MGR:DEV
Quota club trip destined for Hawaii.	EMP:SALES
Source control software updates distributed next week.	EMP:DEV
Firewall attacks increasing.	EMP:IS
Party in Madison Ave. office cancelled	EMP:SALES:NY
Presidential outlook for economy may affect revenue.	MGR:SALES:US
Earthquake preparation team meeting tonight.	EMP:SALES:LA
National Language Support API released.	EMP:DEV:APAC

Testing

- By switching to each authorization, test the authorizations and data labes to ensure the labels ang authorizations are working to your understanding.
- Explain the results.

ALL_EXECS
EXEC:SALES, DEV, IS:CORP

MESSAGE	OLS Label
This message is only for the Executive Staff.	EXEC
All Managers: employee compensation announcement...	MGR
This message is to notify all employees...	EMP
New updates to quotas have been assigned.	MGR:SALES
New product release date meeting scheduled.	MGR:DEV
Quota club trip destined for Hawaii.	EMP:SALES
Source control software updates distributed next week.	EMP:DEV
Firewall attacks increasing.	EMP:IS
Party in Madison Ave. office cancelled	EMP:SALES:NY
Presidential outlook for economy may affect revenue.	MGR:SALES:US
Earthquake preparation team meeting tonight.	EMP:SALES:LA
National Language Support API released.	EMP:DEV:APAC

Testing

US_SALES_MGR
MGR:SALES:US

MESSAGE	OLS Label	
This message is only for the Executive Staff.	EXEC	1
All Managers: employee compensation announcement...	MGR	2
This message is to notify all employees...	EMP	3
New updates to quotas have been assigned.	MGR:SALES	4
New product release date meeting scheduled.	MGR:DEV	5
Quota club trip destined for Hawaii.	EMP:SALES	6
Source control software updates distributed next week.	EMP:DEV	7
Firewall attacks increasing.	EMP:IS	8
Party in Madison Ave. office cancelled	EMP:SALES:NY	9
Presidential outlook for economy may affect revenue.	MGR:SALES:US	10
Earthquake preparation team meeting tonight.	EMP:SALES:LA	11
National Language Support API released.	EMP:DEV:APAC	12

Testing

DEV_MANAGERS
MGR:DEV:CORP

MESSAGE	OLS Label	
This message is only for the Executive Staff.	EXEC	1
All Managers: employee compensation announcement...	MGR	2
This message is to notify all employees...	EMP	3
New updates to quotas have been assigned.	MGR:SALES	4
New product release date meeting scheduled.	MGR:DEV	5
Quota club trip destined for Hawaii.	EMP:SALES	6
Source control software updates distributed next week.	EMP:DEV	7
Firewall attacks increasing.	EMP:IS	8
Party in Madison Ave. office cancelled	EMP:SALES:NY	9
Presidential outlook for economy may affect revenue.	MGR:SALES:US	10
Earthquake preparation team meeting tonight.	EMP:SALES:LA	11
National Language Support API released.	EMP:DEV:APAC	12

Step 5.1: Assign label to user

- **BY USING SA_USER_ADMIN.SET_LEVELS**

```
-- Authorizing levels
sec_mgr> BEGIN
2 sa_user_admin.set_levels
3 (policy_name => 'ESBD',
4 user_name => 'DIRECTOR',
5 max_level => 'EXEC',
6 min_level => 'EMP',
7 def_level => 'EXEC',
8 row_level => 'EXEC');
9 END;
```

```
-- Authorizing compartments
sec_mgr> BEGIN
2 sa_user_admin.set_compartments
3 (policy_name => 'ESBD',
4 user_name => 'DIRECTOR',
5 read_comps => 'SALES,DEV,IS',
6 write_comps => 'SALES,DEV,IS',
7 def_comps => 'SALES,DEV,IS',
8 row_comps => 'SALES,DEV,IS');
9 END;
```

```
-- Authorizing groups
sec_mgr> BEGIN
2 sa_user_admin.set_compartments
3 (policy_name => 'ESBD',
4 user_name => 'DIRECTOR',
5 read_groups => 'CORP',
6 write_groups => 'CORP',
7 def_groups => 'CORP',
8 row_groups => 'CORP');
9 END;
```

B51: Assign label to user

- **Using sa_user_admin.set_user_labels**

```
sa_user_admin.set_user_labels
(policy_name => 'ESBD',
user_name => 'US_SALES_MGR',
     max_read_label => 'MGR:SALES:US');
```

B51: Assign specific authorizations to user

- **Using SA_USER_ADMIN.SET_USER_PRIVS**

```
BEGIN
SA_USER_ADMIN.SET_USER_PRIVS (
policy_name => 'hr_ols_pol',
user_name => 'jgodfrey',
privileges => 'FULL');
END;
/
```

Specific authorizations of OLS

- A user can be granted the pre-defined authorizations of OLS.
- Sec_mgr kích hoạt quyền PROFILE_ACCESS để có thể chuyển đổi profile.
- Some privileges allowed the authorized user to bypass the specific label security enforcements:
  - **PROFILE ACCESS** Allows the user to switch their security profile
  - **READ** Allows the user to select any data. This is valuable for inspecting labels and performing exports of data.
  - **WRITE** Allows the user to override the OLS protections for each of the label components.
  - **FULL** This is the shortcut for granting both read and write privileges.

  The privileges are unique to OLS and only can be enabled by invoking the SA_USER_ADMIN.SET_USER_PRIVS

References

1. Oracle Label Security Administrator's Guide, 12*c* Release 2 (12.2) https://docs.oracle.com/en/database/oracle/oracle-database/12.2/olsag/label-security-administrators-guide.pdf
2. D.C. Knox, Effective Oracle Database 10g Security by Design, Chapter 12, Oracle Press, ISBN 0-07-223130-0, 2004.

B33: Định nghĩa các nhãn

	Label tag	Label value
Nhãn chỉ có level	1	EXEC
	2	MGR
	3	EMP
Nhãn gồm level và compartment	10	EXEC:SALES, DEV, IS
	20	MGR:SALES
	25	MGR:DEV
	30	EMP:SALES
	35	EMP:DEV
	39	EMP:IS
Nhãn gồm level, compartment và group	300	MGR:SALES:EMEA
	310	MGR:SALES:US
	320	EMP:SALES:NY
	330	EMP:SALES:LA
	400	EMP:DEV:US
	410	EMP:DEV:APAC
	450	MGR:DEV:CORP

Q&A

Dr. Phạm Thị Bạch Huệ - ptbhue@fit.hcmus.edu.vn

MSc. Lương Vĩ Minh - lvminh@fit.hcmus.edu.vn