



IBM Software Group

RACF DB2 V8 Row Level Security - User Experiences

Session: E8

Presented by Julie Bergh CISSP CBCP

Certified IBM IT Specialist

jbergh@us.ibm.com



© 2006 IBM Corporation

IBM Software Group



Trademarks

- The following are trademarks or registered trademarks of the International Business Machines Corporation (IBM) or subsidiaries
 - ▶ IBM®, CICS®, DB2®, Tivoli®, zSeries®,
 - ▶ z/OS®, OS/390®, MVS, MVS/ESA, MVS/XA
 - ▶ RACF®, SecureWay®, Security Server
- Microsoft™, Windows, and the Windows logo are trademarks of Microsoft™
- Java™ and all Java-based trademarks are trademarks of Sun Microsystems, Inc.
- UNIX™ is a registered trademark in the United States and other countries licensed exclusively through The Open Group
- Other company, product, and service names may be the trademarks or service marks of others in the United States, other countries, or both



2

Objectives

- User experience on setting up RACF / DB2 V8 / row level security (multilevel security).
- Provide an understanding of what is required from the RACF perspective, high level on considerations from the DB2 perspective, design considerations, and how tested.

Agenda

- Definitions
- Checklist
- References
- Summary

Definitions

- Discretionary Access Control
 - ▶ A means of restricting access to objects based upon the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject
- Mandatory Access Control
 - ▶ A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (e.g., clearance) of subjects to access information of such sensitivity

5

Definitions

- Multilevel security
 - ▶ The ability to mix different categories and classes of information within the same computing environment in a controlled manner without compromise
- Valuable anytime there is a need to isolate data, such as:
 - ▶ In a service bureaus environment
 - ▶ When there is truly sensitive data
 - ▶ As a way of complying with evolving regulatory environment
- Controls / Classifies data using:
 - ▶ Security Levels
 - ▶ Security categories

6

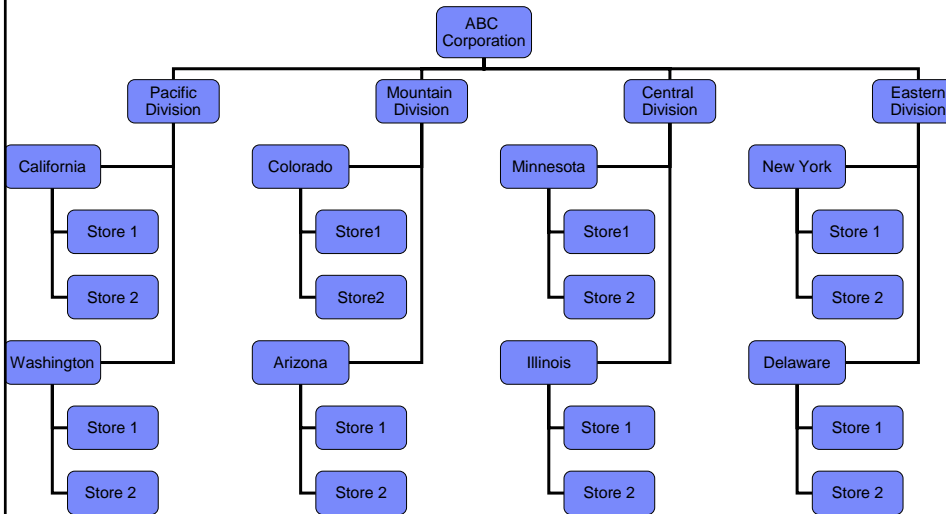
Checklist


✓ Plan

- Create Security Levels (RACF SECLABELS – SECDATA (SECLEVEL and CATEGORY))
- Define SECLABELs to RACF
- Initial Setup for Initial Verification of Process
 - Assign SYSHIGH to Security Administrator (SECURE1) and Database administrator (DBA1)
 - PERMIT SYSHIGH to SECURE1 and DBA1
 - Activate and RACLIST SECLABELs class
 - Log on to TSO ensure would work
 - PERMIT DBA1 and SECURE1 access to various SECLABELs
 - Log on to TSO to test access to these SECLABELs
- Add SECLABEL column to DB2 tables
- Modify SECLABEL column to have correct SECLABEL for application access
- Test access using SQL with various SECLABELs
- Other considerations




ABC Corporation




IBM Software Group 

Store	Inventory #	Description	Price
AZS1	ABC	SHIRT	11.95
AZS2	ABC	SHIRT	11.95
AZS1	DEF	PANT	21.95
AZS2	DEF	PANT	21.95
CAS2	ABC	SHIRT	18.95
CAS1	DEF	PANT	28.95
CAS2	DEF	PANT	28.95
WAS1	ABC	SHIRT	12.95
WAS1	GHI	SHOE	31.95
WAS2	ABC	SHIRT	12.95
COS1	ABC	SHIRT	13.95
COS2	DEF	PANT	23.95
COS2	GHI	SHOE	32.95
MNS1	ABC	SHIRT	14.95
MNS2	ABC	SHIRT	14.95
MNS1	DEF	PANT	24.95
MNS2	GHI	SHOE	33.85

Sample of DB2 Table
At
ABC Corporation




9

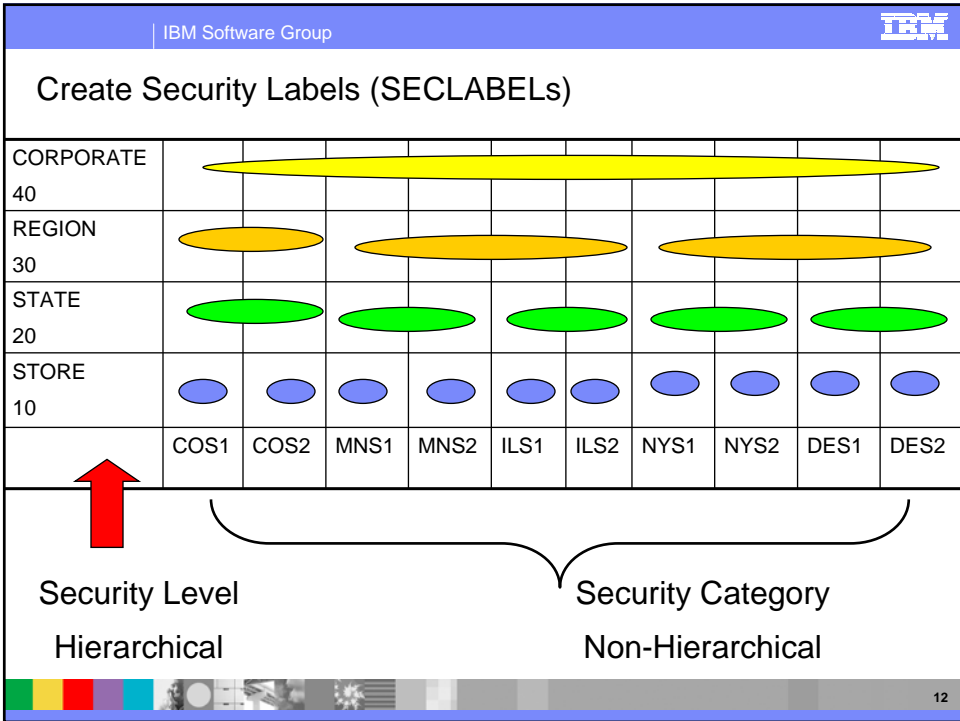
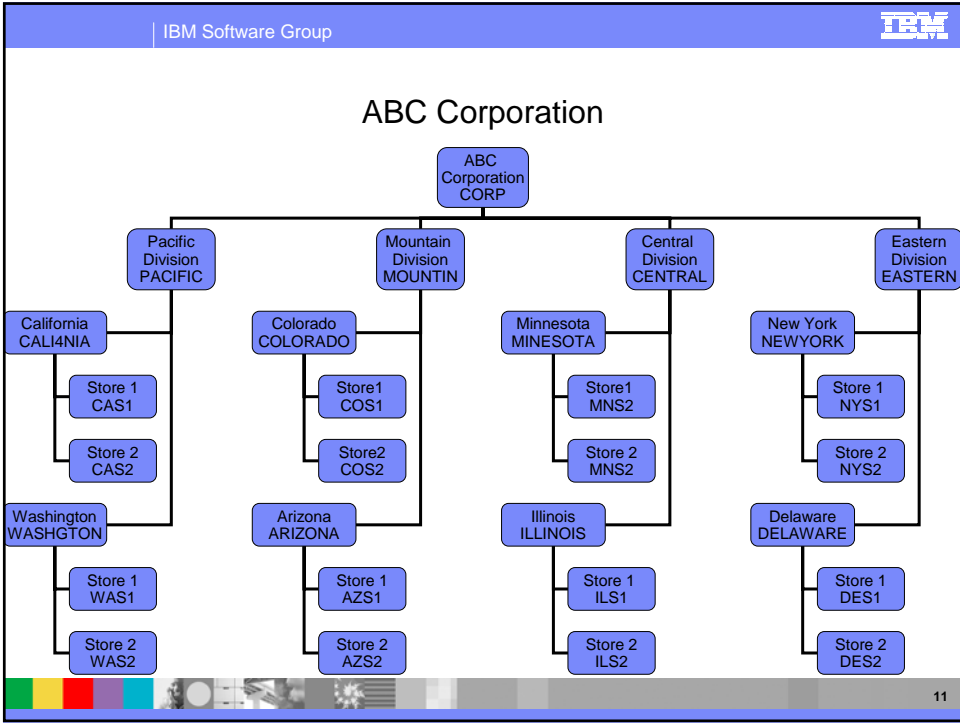
IBM Software Group 

Checklist

- Plan
- Create Security Levels (RACF SECLABELS – SECDATA (SECLEVEL and CATEGORY))
 - Define SECLABELS to RACF
 - Initial Setup for Initial Verification of Process
 - Assign SYSHIGH to Security Administrator (SECURE1) and Database administrator (DBA1)
 - PERMIT SYSHIGH to SECURE1 and DBA1
 - Activate and RACLIST SECLABELS class
 - Log on to TSO ensure would work
 - PERMIT DBA1 and SECURE1 access to various SECLABELS
 - Log on to TSO to test access to these SECLABELS
 - Add SECLABEL column to DB2 tables
 - Modify SECLABEL column to have correct SECLABEL for application access
 - Test access using SQL with various SECLABELS
 - Other considerations



10



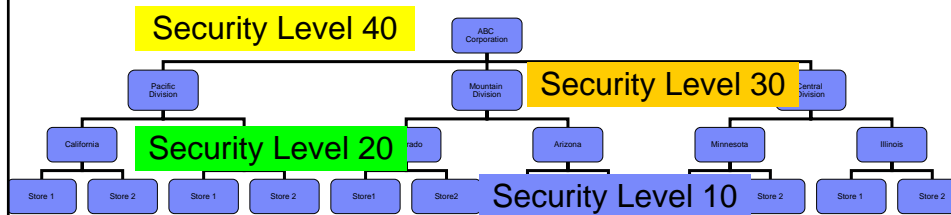
Dominance and Equivalence

- When SECLABELs are compared in an access check, RACF examines the dominance relationship between the SECLABELs.
- For SECLABEL A to dominate SECLABEL B
 - ▶ The Security Level of A is equal to or greater than the Security Level of B
 - ▶ A has at least all the Categories that define B
 - ▶ Avoid the temptation to say that SECLABEL A is “greater” than SECLABEL B
- SECLABELs A and B are equivalent if the A dominates B and B dominates A
 - ▶ Same SECLEVEL
 - ▶ Same set of categories
 - ▶ Equivalence is a ‘subset’ of dominance
- Disjoint SECLABELs are SECLABELs where there is at least one category in SECLABEL A that is not in SECLABEL B and one category in SECLABEL B that is not in SECLABEL A

RACF Checking

- RACF compares the security level allowed in the user profile with the security level required in the resource profile.
- MLS combines hierarchical security levels with nonhierarchical security categories, RACF can return one of four values when comparing security levels:
 - ▶ Dominate (greater than or equal to)
 - ▶ Reverse dominate (less than or equal to)
 - ▶ Equivalence (equal to -- the SECLABELs are the same)
 - ▶ Null (none of the above)

ABC Corporation



We established security labels matching the organization hierarchy — so that a user with the highest security level can access everything and users with lower ratings are limited.

At ABC Corporation a user at the Corporation level has access to all the data

Users at different levels in the organization have their view of the data limited.

You could also establish a hierarchy within the Region by department level or some other characteristic. Note, though, that although security levels are hierarchies, security categories operate as a set.

RACF Security Labels

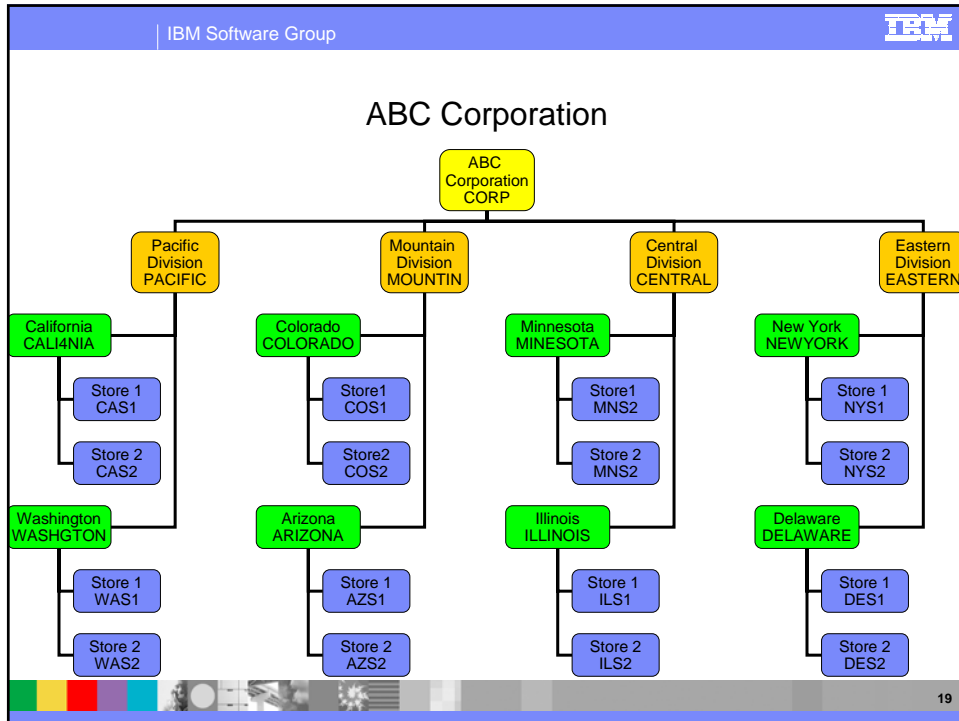
- A security label or SECLABEL consists of two parts:
 - A security level (SECLEVEL)
 - Zero or more security categories
- Security Labels are defined in the SECLABEL class
- In a fully-operational multilevel security environment, all users and data objects must have SECLABELS (NOT at this Corporation)
- SECLABELS can be assigned to users (including started task and batch users), data resources, and to other security-related objects (such as terminals).


Checklist

- ✓ Plan
- ✓ Create Security Levels (RACF SECLABELS – SECDATA (SECLEVEL and CATEGORY))
- ✓ Define SECLABELs to RACF
- Initial Setup for Initial Verification of Process
 - Assign SYSHIGH to Security Administrator (SECURE1) and Database administrator (DBA1)
 - PERMIT SYSHIGH to SECURE1 and DBA1
 - Activate and RACLIST SECLABELs class
 - Log on to TSO ensure would work
 - PERMIT DBA1 and SECURE1 access to various SECLABELs
 - Log on to TSO to test access to these SECLABELs
- Add SECLABEL column to DB2 tables
- Modify SECLABEL column to have correct SECLABEL for application access
- Test access using SQL with various SECLABELs
- Other considerations

Define SECLABELs to RACF

- Security labels are defined in the SECLABEL class (SECLABELs vs. security labels).
- SECLABEL is a combination of security level (the SECLEVEL profile in the SECDATA class), and set of zero or more categories (the CATEGORY profile in the SECDATA class).
- Users are then granted access to any SECLABELs they need authority to.
- Users can only have one SECLABEL active at a time for a session. At logon time, the user can request to log on with any SECLABEL they have authority to. During the life of that session, the user is considered to be at the SECLABEL they logged on with. Resources, such as a data sets, that require a security label are given SECLABELs as well.
- A SECLABEL cannot be assigned to a RACF group; only individual subjects or objects can have security labels assigned to them.
- Authorization to use a security label can be given by permitting a RACF group (to which the user must be connected) READ access to the security label profile in the resource class SECLABEL. Hint: Have the group the same name as the SECLABEL.



IBM Software Group 

Define SECLABELs to RACF

- Security Levels and categories are defined in the SECDATA general resource class

```

AG @MLS SUPGROUP($SYSRES) OWNER($SYSRES)
RDEF SECDATA SECLEVEL UACC(NONE) OWNER(@MLS)
RALT SECDATA SECLEVEL ADDMEM(STORE/10, STATE/20, REGION/30, CORPORATE/40) OWNER(@MLS)
  
```

- The 2 items must be separated by a slash (/). The Name can be up to 44 characters and must not contain a blank, comma, semicolon, right parenthesis. The number can be any number from 1 through 254. The higher the number, the higher the security level.

```

RDEF SECDATA CATEGORY UACC(NONE) OWNER(@MLS)
RALT SECDATA CATEGORY ADDMEM(AZ1, AZ2, CAS1,CAS2, WAS1, WAS2, COS1, COS2, ILS1, ILK2, MNS1, MNS2, NYS1, NYS2, DES1, DES2) OWNER(@MLS)
  
```

20

Define SECLABELs to RACF

```
RDEF SECLABEL CORP SECLEVEL(CORPORATE) ADDCATEGORY(AZ1,
AZ2, CAS1, CAZ2, WAS1, WAS2, COS1, COS2, ILS1, ILK2, MNS1, MNS2,
NYS1, NYS2, DES1, DES2) OWNER(@MLS)
```

```
RDEF SECLABEL PACIFIC SECLEVEL(REGION) ADDCATEGORY( WAS1,
WAS2, CAS1, CAS2) OWNER(@MLS)
```

```
RDEF SECLABEL MOUNTIN SECLEVEL(REGION) ADDCATEGORY(AZS1,
AZS2, COS1, COS2) OWNER(@MLS)
```

```
RDEF SECLABEL CENTRAL SECLEVEL(REGION) ADDCATEGORY(ILS1,
ILS2, MNS1, MNS2) OWNER(@MLS)
```

```
RDEF SECLABEL EASTERN SECLEVEL(REGION) ADDCATEGORY(NYS1,
NYS2, DES1, DES2) OWNER(@MLS)
```

Define SECLABELs to RACF

```
RDEF SECLABEL CALI4NIA SECLEVEL(STATE) ADDCATEGORY(CAS1, CAS2)
OWNER(@MLS)
```

```
RDEF SECLABEL WASHGTON SECLEVEL(STATE) ADDCATEGORY(WAS1, WAS20)
OWNER(@MLS)
```

```
RDEF SECLABEL ARIZONA SECLEVEL(STATE) ADDCATEGORY(AZS1, AZS2)
OWNER(@MLS)
```

```
RDEF SECLABEL COLORADO SECLEVEL(STATE) ADDCATEGORY(COS1, COS2)
OWNER(@MLS)
```

```
RDEF SECLABEL ILLINOIS SECLEVEL(STATE) ADDCATEGORY(ILS1, ILS2)
OWNER(@MLS)
```

```
RDEF SECLABEL MINESOTA SECLEVEL(STATE) ADDCATEGORY(MNS2, MNS1)
OWNER(@MLS)
```

```
RDEF SECLABEL NEWYORK SECLEVEL(STATE) ADDCATEGORY(NYS1, NYS2)
OWNER(@MLS)
```

```
RDEF SECLABEL DELAWARE SECLEVEL(STATE) ADDCATEGORY(DES1, DES2)
OWNER(@MLS)
```

Define SECLABELs to RACF

```

RDEF SECLABEL CAS1 SECLEVEL(STORE) ADDCATEGORY(CAS1) OWNER(@MLS)
RDEF SECLABEL CAS2 SECLEVEL(STORE) ADDCATEGORY(CAS2) OWNER(@MLS)
RDEF SECLABEL WAS1 SECLEVEL(STORE) ADDCATEGORY(WAS1) OWNER(@MLS)
RDEF SECLABEL WAS2 SECLEVEL(STORE) ADDCATEGORY(WAS2) OWNER(@MLS)
RDEF SECLABEL AZS1 SECLEVEL(STORE) ADDCATEGORY(AZS1) OWNER(@MLS)
RDEF SECLABEL AZS2 SECLEVEL(STORE) ADDCATEGORY(AZS2) OWNER(@MLS)
RDEF SECLABEL COS1 SECLEVEL(STORE) ADDCATEGORY(COS1) OWNER(@MLS)
RDEF SECLABEL COS2 SECLEVEL(STORE) ADDCATEGORY(COS2) OWNER(@MLS)
RDEF SECLABEL MNS1 SECLEVEL(STORE) ADDCATEGORY(MNS1) OWNER(@MLS)
RDEF SECLABEL MNS2 SECLEVEL(STORE) ADDCATEGORY(MNS2) OWNER(@MLS)
RDEF SECLABEL ILS1 SECLEVEL(STORE) ADDCATEGORY(ILS1) OWNER(@MLS)
RDEF SECLABEL ILS2 SECLEVEL(STORE) ADDCATEGORY(ILS2) OWNER(@MLS)
RDEF SECLABEL NYS1 SECLEVEL(STORE) ADDCATEGORY(NYS1) OWNER(@MLS)
RDEF SECLABEL NYS2 SECLEVEL(STORE) ADDCATEGORY(NYS2) OWNER(@MLS)
RDEF SECLABEL DES1 SECLEVEL(STORE) ADDCATEGORY(DES1) OWNER(@MLS)
RDEF SECLABEL DES2 SECLEVEL(STORE) ADDCATEGORY(DES2) OWNER(@MLS)

```

23

Checklist

- ✓ Plan
- ✓ Create Security Levels (RACF SECLABELS – SECDATA (SECLEVEL and CATEGORY))
- ✓ Define SECLABELs to RACF
- ✓ Initial Setup for Initial Verification of Process
 - ✓ Assign SYSHIGH to Security Administrator (SECURE1) and Database administrator (DBA1)
 - ✓ PERMIT SYSHIGH to SECURE1 and DBA1
 - ✓ Activate and RACLIST SECLABELs class
 - ✓ Log on to TSO ensure would work
 - ✓ PERMIT DBA1 and SECURE1 access to various SECLABELs
 - ✓ Log on to TSO to test access to these SECLABELs
- Add SECLABEL column to DB2 tables
- Modify SECLABEL column to have correct SECLABEL for application access
- Test access using SQL with various SECLABELs
- Other considerations

24

Initial Verification Process

ALU SECURE1 SECLABEL(SYSHIGH)

ALU DBA1 SECLABEL(SYSHIGH)

- Assigning a **SECLABEL** to a user does not give the user access to the **SECLABEL**. The user must be **PERMITTED** to the **SECLABEL**

PE SYSHIGH CLASS(SECLABEL) ID(SECURE1) ACCESS(READ)

PE SYSHIGH CLASS(SECLABEL) ID(DBA1) ACCESS(READ)

SECLABEL class must be **RACLISTed**

SETR CLASSACT(SECLABEL) RACLIST(SECLABEL)

Log on to TSO and will see SECLABEL filled in screen

RACF Defined SECLABELs

- RACF provides several system-defined SECLABELs
 - ▶ **SYSNONE** – Combines the lowest Security Level and NO Categories
 - ▶ **SYLOW** – Combines the lowest Security Level and NO Categories
 - ▶ **SYSHIGH** – Combines the highest Security Level and ALL Categories
 - ▶ **SYSMULTI** - Label is considered to be equivalent to *any* defined security label. Not generally appropriate for users.
- Activating SECLABELs alters the access check path:
 - ▶ If the both the user and the object have a SECLABEL then the user's SECLABEL is compared to the resource
 - ▶ If the resource has a SECLABEL and the user does not, then the access check fails.
 - ▶ If the user has a SECLABEL and but the resource does not, then the access check continues with the discretionary access check

Checklist

- ✓ Plan
- ✓ Create Security Levels (RACF SECLABELS – SECDATA (SECLEVEL and CATEGORY))
- ✓ Define SECLABELs to RACF
- ✓ Initial Setup for Initial Verification of Process
 - ✓ Assign SYSHIGH to Security Administrator (SECURE1) and Database administrator (DBA1)
 - ✓ PERMIT SYSHIGH to SECURE1 and DBA1
 - ✓ Activate and RACLIST SECLABELs class
 - ✓ Log on to TSO ensure would work
 - ✓ PERMIT DBA1 and SECURE1 access to various SECLABELs
 - ✓ Log on to TSO to test access to these SECLABELs
- ✓ Add SECLABEL column to DB2 tables
- Modify SECLABEL column to have correct SECLABEL for application access
- Test access using SQL with various SECLABELs
- Other considerations

27

DB2 Checklist – High Level

- Use SECLABELs
- Table has a column defined as a security label
- Each row value has a specific security label
- Get user security label from RACF
- Save in rows for INSERT, UPDATE, LOAD, ...
- Compare SECLABEL in row to SECLABEL for the DB2 users
- If access is allowed, then normal access
- If access is not allowed, data not returned
- Runtime user to data checking
- Seclabel values are cached to minimize processing time

28

DB2 / MLS

- With MLS providing row-level granularity, applications can access DB2 data without using special views.
- When you CREATE a table or ALTER it, you can decide to implement row-level security by including a column that specifies the AS SECURITY LABEL attribute, or add a column with that attribute to an existing table.
- To disable row level security (a table that has a column that is defined with the AS SECURITY LABEL attribute) is to drop the table, table space, or database.



Store	Inventory #	Description	Price	Seclabel
AZS1	ABC	SHIRT	11.95	SYSHIGH
AZS2	ABC	SHIRT	11.95	SYSHIGH
AZS1	DEF	PANT	21.95	SYSHIGH
AZS2	DEF	PANT	21.95	SYSHIGH
CAS2	ABC	SHIRT	18.95	SYSHIGH
CAS1	DEF	PANT	28.95	SYSHIGH
CAS2	DEF	PANT	28.95	SYSHIGH
WAS1	ABC	SHIRT	12.95	SYSHIGH
WAS1	GHI	SHOE	31.95	SYSHIGH
WAS2	ABC	SHIRT	12.95	SYSHIGH
COS1	ABC	SHIRT	13.95	SYSHIGH
COS2	DEF	PANT	23.95	SYSHIGH
COS2	GHI	SHOE	32.95	SYSHIGH
MNS1	ABC	SHIRT	14.95	SYSHIGH
MNS2	ABC	SHI		
MNS1	DEF	PA		
MNS2	GHI	SH		

DB2 Table with
SECLABEL Column
Added

SECLABEL defaults
to SYSHIGH

```
ALTER TABLE STORE.EXP
ADD CLASSIFICATION CHAR(8) FOR SBCS DATA
NOT NULL WITH DEFAULT
AS SECURITY LABEL;
```



Add SECLABEL to DB2 Table – CREATE/ALTER

- Table must have a column assigned to store the SECLABEL - to define a column as the security label column
- Security label column can have any column name
- Specify "AS SECURITY LABEL" as the column attribute.
 - You can assign any name to the security label column, but the same column name cannot be used more than once in the table. Only one security label is allowed per table.
 - This indicates that the table is defined with multilevel security with row granularity.
 - The column should have the attribute data type single byte character (SBCS), CHAR(8)
 - NOT NULL WITH DEFAULT
 - Cannot be a column with Fieldproc, editproc, or check constraint
- Table once created with SECLABEL cannot be disabled
- Audit record produced if the table with security label is created, altered or dropped

Store	Inventory #	Description	Price	Seclabel
AZS1	ABC	SHIRT	11.95	AZS1
AZS2	ABC	SHIRT	11.95	AZS2
AZS1	DEF	PANT	21.95	AZS1
AZS2	DEF	PANT	21.95	AZS2
CAS2	ABC	SHIRT	18.95	CAS2
CAS1	DEF	PANT	28.95	CAS1
CAS2	DEF	PANT	28.95	CAS2
WAS1	ABC	SHIRT	12.95	WAS1
WAS1	GHI	SHOE	31.95	WAS1
WAS2	ABC	SHIRT	12.95	WAS2
COS1	ABC	SHIRT	13.95	COS1
COS2	DEF	PANT	23.95	COS2
COS2	GHI	SHOE	32.95	COS2
MNS1	ABC	S		
MNS2	ABC	S		
MNS1	DEF	E		
MNS2	GHI	S		

DB2 Table with
Correct
SECLABELS
Defined

Example SQL to update SECLABEL

```
UPDATE STORE.EXP
SET CLASSIFICATION = 'AZS1' WHERE STORE =
'AZS1';
```


Store	Inventory #	Description	Price	Seclabel
WAS1	ABC	SHIRT	12.95	WAS1
WAS1	GHI	SHOE	31.95	WAS1

SELECT

SQL by user to access data

- Employee Joe runs SQL to access Data
- Joe has SECLABEL WAS1

```
SELECT
STORE,INVENTORY,DESCRIPTION,PRICE
FROM STORE.EXP;
```

- Joe's SECLABEL compared to SECLABEL of row
- If Joe's SECLABEL dominates the data SECLABEL
 - Row is returned
- If Joe's SECLABEL does not dominate the data SECLABEL
 - Row is not returned, but no error is reported

SQL With SELECT

- The security rule for select is that your current security label must dominate the security label of all the rows read. If your security label does not dominate the label of the data row, then that row is not returned.
- The user must be identified to RACF with a valid SECLABEL. If not, an authorization error and audit record (IFCID 140) are produced, provided the audit trace is active.
- DB2 ignores rows that the user doesn't have access to, and doesn't report an error. Using MLS means that only the records the user can access are processed (rather than all the qualifying records in a table).

Checklist

- ✓ Plan
- ✓ Create Security Levels (RACF SECLABELS – SECDATA (SECLEVEL and CATEGORY))
- ✓ Define SECLABELs to RACF
- ✓ Initial Setup for Initial Verification of Process
 - ✓ Assign SYSHIGH to Security Administrator (SECURE1) and Database administrator (DBA1)
 - ✓ PERMIT SYSHIGH to SECURE1 and DBA1
 - ✓ Activate and RACLIST SECLABELs class
 - ✓ Log on to TSO ensure would work
 - ✓ PERMIT DBA1 and SECURE1 access to various SECLABELs
 - ✓ Log on to TSO to test access to these SECLABELs
- ✓ Add SECLABEL column to DB2 tables
- ✓ Modify SECLABEL column to have correct SECLABEL for application access
- ✓ Test access using SQL with various SECLABELs
- ✓ Other considerations

DB2 INSERT / UPDATE Row

- INSERT
 - ▶ The value of the SECLABEL column for inserted row is set to the value of the user's SECLABEL.
 - ▶ If user has authority for Write-Down, the user is allowed to set the SECLABEL field to any value.
 - ▶ If user does not have authority for Write-Down, the SECLABEL of the inserted rows will be set to current SECLABEL.
- UPDATE
 - ▶ User's SECLABEL compared with the SECLABEL of the row to be updated.
 - ▶ If the SECLABELs are equivalent -- Row is updated and value id determined by whether the user has write-down privileges
 - If the user has write-down privilege or write-down control is not enabled, the user can set the security label of the row to any valid security label.
 - If the user does not have write-down privilege and write-down control is enabled, the security label of the row is set to the value of the security label of the user.

DB2 DELETE Row

- The user must be identified to RACF with a valid SECLABEL. If not, an authorization error and an audit record are produced.
- User's SECLABEL compared with the SECLABEL of the row to be deleted.
- If the security label of the user and the security label of the row are equivalent, the row is deleted.
- If the security label of the user dominates the security label of the row, the user's write-down privilege determines the result of the DELETE statement:
 - ▶ If the user has write-down privilege or write-down control is not enabled, the row is deleted.
 - ▶ If the user does not have write-down privilege and write-down control is enabled, the row is not deleted.
- If the security label of the row dominates the security label of the user, it is not considered a matching row, and the row is not deleted.

DB2 Utilities

- The MLS rules for utilities are similar to those for SQL operations, as follows:
 - ▶ LOAD RESUME rules are similar to INSERT rules.
 - ▶ LOAD REPLACE requires write-down authority because it deletes all rows.
 - ▶ UNLOAD and REORG UNLOAD EXTERNAL rules are similar to SELECT rules.
 - ▶ REORG DISCARD rules are similar to DELETE rules.
- You can use row-level access controls with native DB2 or with RACF access controls.
- If you use RACF access controls, you can define multilevel security for other objects.

DB2 Security Labels and Performance

- The security label column is used whenever a table with multilevel security enabled is accessed.
 - ▶ Include the SECLABEL column in your existing indexes, especially when your queries are using index-only access today.
- DB2 caches security labels (per commit scope) to avoid extra calls to RACF.
- DB2 performs multilevel security with row-level granularity by comparing the security label of the user to the security label of the row that is accessed. Because security labels can be equivalent without being identical, DB2 uses the RACROUTE REQUEST=DIRAUTH macro to make this comparison when the two security labels are not the same. For read operations, such as SELECT, DB2 uses ACCESS=READ. For update operations, DB2 uses ACCESS=READWRITE.
- System allows the definition of several thousand categories (up to 254 security levels) and unlimited security labels. Define only as many as you REALLY need. A large number of levels and categories can decrease performance (particularly at IPL time) and for the SETROPTS RACLIST(REFRESH) command.

Summary

- PLAN, PLAN, PLAN**
- Define environment and SECLABELs**
- Determine initial testing**
- Test**

References

- Security Server (RACF) publications:
 - ▶ RACF Command Language Reference (SC28-1919)
 - ▶ RACF Security Administrator's Guide (SC28-1915)
 - ▶ RACF Callable Services Guide (SC28-1921)
- z/OS publications:
 - ▶ Planning for Multilevel Security (GA22-7509-00)
- RACF web site:
 - ▶ <http://www.ibm.com/servers/eserver/zseries/zos/racf>
- Redbook:
 - ▶ Multilevel Security and DB2 Row-Level Security Reveled (SG24-6480-00)
- DB2 web site:
 - ▶ <http://www.ibm.com/software/db2zos>
- Related publications / presentations:
 - ▶ <http://www.ibm.com/software/db2zos/db2zosv8.html>
 - ▶ <http://www.ibm.com/software/db2zos/presentations.html>
 - ▶ <http://www.ibm.com/software/db2zos/support.html>

Questions

