An Expert Guide to New SAP BI Security Features

Marc Bernard
SAP Labs
Objectives

In this session you will …

- Learn how to grant access to data on various levels of detail
- Find out how the new analysis authorizations compare to the old concept based on authorization objects
- Understand the new options for defining authorizations
- See a demonstration of the new functionality
- Hear about migration tools
- Take away information about the latest monitoring and auditing capabilities for security settings
Overview of New Authorization Concept
Comparison of Old and New Authorization Concepts
Authorization Maintenance
Generating Authorizations Automatically
Assigning Authorizations to Users and Roles
Monitoring, Auditing, and Test Tools
Migration
Summary
Overview of New Authorization Concept

Comparison of Old and New Authorization Concepts

Authorization Maintenance

Generating Authorizations Automatically

Assigning Authorizations to Users and Roles

Monitoring, Auditing, and Test Tools

Migration

Summary
Application Security

- Based on roles and authorization concept
- Users are assigned to roles
- Roles contain authorizations
- Authorizations are defined for authorization objects
- The system checks authorization objects against the authorizations of the user
Comparison of OLTP and OLAP Security Needs

Security Needs in mySAP ERP (OLTP)

- Transaction-based security
- Driven by:
  - Transaction codes
  - Specific field values
  - Which activities a user can perform
- Focused on getting daily work completed as quickly and efficiently as possible

Security Needs in SAP NetWeaver BI (OLAP)

- Analysis-based security
- Driven by:
  - InfoProviders
  - Queries
  - Data
- Different business purpose and goals than OLTP
- Focused on displaying, planning, and analyzing data
Terminology

Standard Authorizations
- Based on standard role and authorization concept of SAP
- Was and still are used for BI administrator and developer activities

Reporting Authorizations
- Old security concept up to SAP NetWeaver ’04 (up to SAP BW 3.5)
- Control for which data a user has access to in a query
- Realized through the standard authorization concept, which has many limitations

Analysis Authorizations
- New security concept as of SAP NetWeaver 2004s
- Is not based on standard authorization concept in order to overcome the limitations
- Takes features of reporting and analysis in BI into consideration
Scenario: Sufficient Authorizations

- Complete selection is subset of authorizations
  - Query results will be shown

Scenario: Insufficient Authorizations

- Complete or part of selection is outside of authorizations
  - Query results will not be shown at all
Exceptions for “All-or-Nothing” Rule

- Display hierarchies are automatically filtered by the authorization
- Key figure values are not displayed if the key figure is not authorized
Authorization Levels

Access Can Be Restricted by Authorizations ...

- On InfoCube Level
- On Characteristic Level
- On Characteristic Value Level
- On Key Figure Level
- On Hierarchy Node Level

- On Characteristic Value Level

- On Key Figure Level
<table>
<thead>
<tr>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of New Authorization Concept</td>
</tr>
<tr>
<td>Comparison of Old and New Authorization Concepts</td>
</tr>
<tr>
<td>Authorization Maintenance</td>
</tr>
<tr>
<td>Generating Authorizations Automatically</td>
</tr>
<tr>
<td>Assigning Authorizations to Users and Roles</td>
</tr>
<tr>
<td>Monitoring, Auditing and Test Tools</td>
</tr>
<tr>
<td>Migration</td>
</tr>
<tr>
<td>Summary</td>
</tr>
</tbody>
</table>
Limitations of earlier SAP BW releases

<table>
<thead>
<tr>
<th>Technical Foundation</th>
<th>&lt;=SAP BW 3.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance</td>
<td>Authorization objects</td>
</tr>
<tr>
<td>Number of InfoObjects</td>
<td>Not changeable afterwards</td>
</tr>
<tr>
<td>Navigational Attributes</td>
<td>Ten InfoObjects</td>
</tr>
<tr>
<td>Hierarchy Authorizations</td>
<td>Only on global basis</td>
</tr>
<tr>
<td>Composition of Authorizations</td>
<td>Via GUID and 0TCTAUTHH</td>
</tr>
<tr>
<td>Authorization Relevance</td>
<td>Only intersection of auth. objects permitted</td>
</tr>
<tr>
<td>Validity</td>
<td>Per InfoObject AND InfoCube</td>
</tr>
<tr>
<td>InfoProvider Authorizations</td>
<td>Tied to role only</td>
</tr>
<tr>
<td></td>
<td>Separate authorization objects (S_RS_*)</td>
</tr>
</tbody>
</table>
## Comparing Authorization Concepts (cont.)

### Improvements with SAP NetWeaver 2004s

<table>
<thead>
<tr>
<th></th>
<th>&lt;=SAP BW 3.x</th>
<th>SAP NetWeaver 2004s</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Foundation</strong></td>
<td>Authorization objects</td>
<td>Analysis authorization</td>
</tr>
<tr>
<td></td>
<td>Not changeable afterwards</td>
<td>Changeable</td>
</tr>
<tr>
<td><strong>Maintenance</strong></td>
<td>Ten InfoObjects</td>
<td>Number of InfoObjects not limited</td>
</tr>
<tr>
<td><strong>Number of InfoObjects</strong></td>
<td>Only on global basis</td>
<td>Individually</td>
</tr>
<tr>
<td><strong>Navigational Attributes</strong></td>
<td>Via GUID and 0TCTAUTHH</td>
<td>Equivalent to value authorizations</td>
</tr>
<tr>
<td><strong>Hierarchy Authorizations</strong></td>
<td>Only intersection of auth. objects permitted</td>
<td>Union “as expected”</td>
</tr>
<tr>
<td><strong>Composition of Authorizations</strong></td>
<td>Per InfoObject AND InfoCube</td>
<td>Only InfoObject setting</td>
</tr>
<tr>
<td><strong>Authorization Relevance</strong></td>
<td>Tied to role only</td>
<td>Flexible per authorization</td>
</tr>
<tr>
<td><strong>Validity</strong></td>
<td>Separate authorization objects (S_RS_*)</td>
<td>Included in authorization</td>
</tr>
<tr>
<td><strong>InfoProvider Authorizations</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Comparing Authorization Concepts (cont.)

Please see the appendix on your take-home CD for a detailed comparison
Overview of New Authorization Concept
Comparison of Old and New Authorization Concepts
Authorization Maintenance
Generating Authorizations Automatically
Assigning Authorizations to Users and Roles
Monitoring, Auditing, and Test Tools
Migration
Summary
Steps of Authorization Maintenance

Follow these steps to create your authorizations

InfoObject Maintenance (RSD1):

1. Define Authorization-Relevant Characteristics
2. Define Authorization-Relevant Attributes

Management of Analysis Authorizations (RSECADMIN):

3. Authorize Characteristic Values
4. Authorize Attribute Values
5. Authorize Hierarchies
6. Add Special Authorization Characteristics
7. Add Key Figure Authorizations
8. Add Variables in Authorizations
Before you get started, here are some tips:

- Activate all Business Content related to authorizations before you get started
  - InfoObjects: 0TCA* (and 0TCT* if not done already)
  - InfoCubes: 0TCA*

- Set the following InfoObjects as “authorization-relevant”
  - 0TCAACTVT
  - 0TCAIPROV
  - 0TCAVALID
  - 0TCAKYFNM

- Add 0TCAIFAREA as an external hierarchy characteristic to 0INFOPROV
Before restricting authorizations on characteristics, you have to mark them as authorization-relevant.
If you want to grant authorizations on navigational attributes, mark them in the attribute tab strip as authorization-relevant.
3. Authorizing Characteristic Values

Central maintenance for (analysis) authorizations/transaction RSECAADMIN

Scenario: A group of users is authorized only to specific sales organizations (e.g., Berlin and Birmingham)
A group of users is authorized only to specific sales organizations (e.g., Berlin and Birmingham)

Possible Values

- EQ: Single value
- BT: Range of values
- CP: Contains (simple) patterns ending with * (e.g., XY*)
Special Authorization Values (for all characteristics)

* (asterisk)
- Denotes a set of arbitrary characters
- Used alone to grant access to all values
- Used at the end of a value to specify a simple pattern (example: SAP*)

: (colon)
- Allows access only to aggregated data (e.g., allows information on all sales areas only on aggregated level – not on particular sales areas)

+ (plus)
- Denotes exactly one character
- Used at the end of a value to specify a simple pattern (example: RED+)
- Used to specify date patterns (only for Validity (0TCAVALID))

# (hash)
- Stands for the initial or unassigned value
Navigational Attributes

- Can be assigned individually
- Tip: The referencing characteristic (here: 0D_SALE_ORG) does not need to be authorization-relevant
5. Authorizing Hierarchies

In the same way as with value authorization, you can also grant authorizations on hierarchy levels.

Assume you’ll have a sales organization as depicted.

Hierarchy 'Sales Organisation' Change: 'Modified Version'
5. Authorizing Hierarchies (cont.)

Now you grant access for the complete Americas and France.

You can also use variables to flexibly and dynamically determine hierarchy nodes.
5. Authorizing Hierarchies (cont.)

Type of Authorization

- Only the selected nodes
- Subtree below nodes
- Subtree below nodes to level (incl.)
- Complete hierarchy
- Subtree below nodes to (and including) level (relative)

Use case: Hierarchies that happen to be restructured regularly
5. Authorizing Hierarchies (cont.)

Validity Range

Which authorization hierarchy is checked against the currently used hierarchy (strictness of check)?

- Name, Version Identical, and Key Date Less Than or Equal to
- Name and Version Identical
- Name Identical
- All Hierarchies

**Recommendation:** Try to be as strict as possible!
6. Special Authorization Characteristics

Authorizations on Special Characteristics

Some special characteristics can be included in an authorization. Note: They must not be included in queries!

These special characteristics **must** be assigned to a user in at least one authorization

- InfoProvider
- Validity
- Activity

[Image: Maintain Authorizations: PM_SLSORG_B Edit]

Insert special characteristics
**Recommendation**

It is not technically necessary to include these special characteristics in every authorization, but it is considered a **best practice** in order to retain clarity.
6. Special Authorization Characteristics (cont.)

InfoProvider

- Grant authorization to particular InfoProviders
- Technical name: 0TCAIPROV
- Possible values:
  - Single value (EQ) One InfoProvider
  - Range (BT) Range of InfoProviders
  - Pattern (CP) Selection of InfoProviders (e.g., 0SD_*)
  - Hierarchy node Selection of InfoProviders based on InfoArea hierarchy
- Default * All InfoProviders
Validity

- Define when authorizations are valid or not valid
- Technical name: 0TCAVALID
- Possible values
  - Include (I): Grant authorization
  - Exclude (E): Deny authorization
  - Single value (EQ): Exactly one date
  - Range (BT): Range of dates
  - Less or Equal (LE): Everything <= value in FROM field
  - Greater Than (GT): Everything > value in FROM field
  - Greater or Equal (GE): Everything >= value in FROM field
  - Less Than (LT): Everything < value in FROM field
  - Pattern (CP): Selection of dates
    - (+): denotes exactly one character (e.g., 01.++.2005 until 10.++.2005: allows access only the first 10 days of each month in 2005)
- Default
  - *: Always valid

^ Exclude (E), special ranges (LE, GT, GE, LT), and the plus pattern (+) work ONLY for this special characteristic!
Activity

- Grant authorization to different activities
- Technical name: 0TCAACTVT
- Possible values:
  - 02 Change data (for example, for business planning)
  - 03 Display data
- Default
  - 03 Display data
Key Figure Authorizations

- Grant authorization to particular key figures
- Technical name: 0TCAKYFNM
- Possible values
  - Single value (EQ): Exactly one key figure
  - Range (BT): Selection of key figures
  - Pattern (CP): Selection of key figures based on pattern
- Default
  - *: All key figures
- Tip: If a particular key figure is defined as authorization-relevant, it will be checked for every InfoProvider
8. Variables in Authorizations

Variables of Type “Customer Exit”

- For value and/or hierarchy authorizations
- Determined during query runtime using custom code
- Example: Determine sales organization from assignments of the user master data

Use enhancement RSR00001 (transaction CMOD) for the necessary coding
Overview of New Authorization Concept
Comparison of Old and New Authorization Concepts
Authorization Maintenance
Generating Authorizations Automatically
Assigning Authorizations to Users and Roles
Monitoring, Auditing, and Test Tools
Migration
Summary
Steps for Generating Authorizations

Follow these steps to generate authorizations automatically:

Data Warehouse Workbench (RSA1):
1. Activate Business Content
2. Load DataStore Objects

Management of Analysis Authorizations (RSECADMIN):
3. Generate Authorizations
4. View Generation Log

Tip: Especially with high user counts or very detailed authorizations, generating authorizations will save a lot of manual work
1. Activate Business Content

Business Content for Authorizations

- SAP delivers Business Content for storing authorizations and user assignment of authorizations

- **Human Resources (HR)**

<table>
<thead>
<tr>
<th>ID</th>
<th>Obj. Name</th>
<th>Long Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTCA_DS01</td>
<td>Template for ODS with Authorization Data (Values)</td>
<td></td>
</tr>
<tr>
<td>OTCA_DS02</td>
<td>Template for ODS with Authorization Data (Hierarchy)</td>
<td></td>
</tr>
<tr>
<td>OTCA_DS03</td>
<td>Template for ODS with Description Text Authorizations</td>
<td></td>
</tr>
<tr>
<td>OTCA_DS04</td>
<td>Template for ODS with Assignment of User Authorization</td>
<td></td>
</tr>
<tr>
<td>OTCA_DS05</td>
<td>Template for ODS for Generating Users for Authorizations</td>
<td></td>
</tr>
</tbody>
</table>

- **Controlling (CO)**

<table>
<thead>
<tr>
<th>ID</th>
<th>Obj. Name</th>
<th>Long Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCCA_001</td>
<td>CO-OM-CCA: User Authorizations (Single Values)</td>
<td></td>
</tr>
<tr>
<td>OCCA_002</td>
<td>CO-OM-CCA: User Authorizations (Hierarchy Nodes)</td>
<td></td>
</tr>
<tr>
<td>OCCA_003</td>
<td>CO-OM-CCA: User for Reporting</td>
<td></td>
</tr>
</tbody>
</table>
2. Load DataStore Objects

DataStore Objects for Authorizations

- Fill the DataStore objects with the user data and authorizations
- Extract the data, for example, from an SAP R/3 source system
  or
- Load the data from a flat file

**Tip:** You might want to add some consistency checks here to avoid errors during the generation later
3. Generate Authorizations

Generation of Authorizations from DataStore Objects

- Start the generation by specifying the relevant DataStore objects

Management of Analysis Authorizations

Generating Authorizations in BI from Data in the InfoProviders

<table>
<thead>
<tr>
<th>DS Objects with Authorization Data for</th>
<th>OTCA_DS01</th>
<th>OTCA_DS02</th>
<th>OTCA_DS03</th>
<th>OTCA_DS04</th>
<th>OTCA_DS05</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flat Authorizations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hierarchy Authorizations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorization Texts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorized User Assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User to Be Generated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Start Generation
4. View Generation Log

After the generation is complete, you can view a detailed log:
- First check errors, then also look at warnings.
<table>
<thead>
<tr>
<th>Overview of New Authorization Concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparison of Old and New Authorization Concepts</td>
</tr>
<tr>
<td>Authorization Maintenance</td>
</tr>
<tr>
<td>Generating Authorizations Automatically</td>
</tr>
<tr>
<td><strong>Assigning Authorizations to Users and Roles</strong></td>
</tr>
<tr>
<td>Monitoring, Auditing and Test Tools</td>
</tr>
<tr>
<td>Migration</td>
</tr>
<tr>
<td>Summary</td>
</tr>
</tbody>
</table>
Steps for Assigning Authorizations to Users

Pick one of these options to assign authorizations to users:

Management of Analysis Authorizations (RSECADMIN):

1. Assign Individual Authorizations
2. Assign Groups of Authorizations

Role Maintenance (PFCG):

3. Assign Authorizations to Roles

Tip: You can use a combination of these options. If you already have a role-based infrastructure in place, option 3 will be the best.
1. Assigning Individual Authorizations

Direct Assignment of Authorizations to Users

Management of Analysis Authorizations

- Select a user ID and change the assignment
- Then insert individual authorizations to the assigned list
You can group authorizations into a hierarchy. Use InfoObject 0TCTAUTH for this hierarchy (you’ll have to activate the content objects for this InfoObject).

Then you can assign one or several authorization groups to the selected user.
Special Authorization

Generated Special Authorization: 0BI_ALL

- Automatically generated and not changeable
- Grants authorizations for all values of all authorization-relevant characteristics
- Adjusted whenever a new InfoObject is set to authorization-relevant
- Simple possibility to grant authorizations to everything (e.g., via role – see next slide)
3. Assigning Authorizations to Roles

Role Maintenance

- Alternatively to the direct assignment, you can also assign authorizations to roles, which can then be assigned to users.
- Use authorization object S_RS_AUTH for the assignment of authorizations to roles.
- Maintain the authorizations as values for field BIAUTH.

Image of SAP management and change role: Authorizations with field values for BI Analysis Authorizations in Role and BI Analysis Authorizations.
Overview of New Authorization Concept
Comparison of Old and New Authorization Concepts
Authorization Maintenance
Generating Authorizations Automatically
Assigning Authorizations to Users and Roles
Monitoring, Auditing, and Test Tools
Migration
Summary
Use these tools for monitoring, auditing, and testing authorizations:

1. Authorization Monitoring
2. Legal Audit

Tip: The improved monitoring capabilities are especially helpful for production support
1. Authorization Monitoring

Checking Authorizations

- Log on with your own user ID (production support role)
- Check query execution with the authorizations of a specific user

Tip: There is no password required. Therefore, access to this support tool should be restricted using authorization object S_RSEC.
1. Authorization Monitoring (cont.)

Evaluate Log Protocol

- Turn on logging of user activities related to analysis authorizations
- View detailed information about authorization checks
  - Which characteristics are relevant?
  - Which selections are checked vs. which authorizations?
  - And much more ...

Management of Analysis Authorizations

Log Management Analysis Authorizations

© SAP AG 2006, 51
2. Legal Auditing

Recording of Changes

- Activate the following VirtualProviders from the Business Content (VAL = Values, HIE = Hierarchies, UA = User Assignment)

<table>
<thead>
<tr>
<th>ID</th>
<th>Object Name</th>
<th>Long Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTCA_HIE</td>
<td></td>
<td>Change Document Analysis Authorization</td>
</tr>
<tr>
<td>OTCA_UA</td>
<td></td>
<td>Change Document Authorizations</td>
</tr>
<tr>
<td>OTCA_VAL</td>
<td></td>
<td>Change Document Analysis Authorization</td>
</tr>
</tbody>
</table>

- The system records all changes to authorizations and user assignments

- Using a query, you can easily answer questions like:
  - How many users have access to a given InfoCube?
  - Which users have access to company code 1000?
  - When was authorization GIVEMEALL created, and by whom?
2. Legal Auditing (cont.)

Recording of Changes

- Query Example

<table>
<thead>
<tr>
<th>Date</th>
<th>Authorization (Tech)</th>
<th>InfoObject</th>
<th>Last Changed By</th>
<th>Number of Authorization Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>02.07.2006</td>
<td>RSP_00007060</td>
<td>BRSA/0VCA_NC1</td>
<td>BR90/0HNFE</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRSA/0VCA_NC1.0VCA_NC2</td>
<td>BR90/0HNFE</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRSA/0VCA_NC2</td>
<td>BR90/0HNFE</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRSA/0VCA_NC2R</td>
<td>BR90/0HNFE</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSP_00007071</td>
<td>BR90/0HNFE</td>
<td>16</td>
</tr>
<tr>
<td>03.07.2006</td>
<td>OBJ_ALL</td>
<td>BRSA/0APO_LOCDNO</td>
<td>BR90/0LKE</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRSA/0CALLENDAR</td>
<td>BR90/0LKE</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRSA/0COSTCENTER</td>
<td>BR90/0LKE</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRSA/0COUNTRY</td>
<td>BR90/0LKE</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRSA/0D_CUSTOMER</td>
<td>BR90/0LKE</td>
<td>1</td>
</tr>
</tbody>
</table>

- Linked into Administration Cockpit
<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of New Authorization Concept</td>
</tr>
<tr>
<td>Comparison of Old and New Authorization Concepts</td>
</tr>
<tr>
<td>Authorization Maintenance</td>
</tr>
<tr>
<td>Generating Authorizations Automatically</td>
</tr>
<tr>
<td>Assigning Authorizations to Users and Roles</td>
</tr>
<tr>
<td>Monitoring, Auditing, and Test Tools</td>
</tr>
<tr>
<td>Migration</td>
</tr>
<tr>
<td>Summary</td>
</tr>
</tbody>
</table>
Steps for Migration of Authorizations

Follow these four steps to migrate authorizations:

Migration Tool (program RSEC_MIGRATION):

1. Select Users
2. Select Authorizations
3. Pick Assignment Method
4. Set Migration Mode

Tip: Allocate enough time to do the migration during your system upgrade and for performing thorough tests
Migration Support

- The migration is a singular event (i.e., not to be scheduled later)
- During migration to the new authorization concept, the existing concept won’t be changed
- Semi-automatic migration
  - The more complex the existing authorization concept, the more manual migration work might be necessary
  - Customer-exit variables for 0TCTAUTHH cannot be migrated; the respective hierarchy nodes must be assigned manually
  - Intensive tests are highly recommended
Before You Start (cont.)

Recommendations

- It is highly recommended to migrate to the new concept
- The former authorization concept won’t be supported any longer
- You can, however, switch back to the former concept – in some exceptional cases (IMG setting)
Start the Migration

Migration Step 0

- Run ABAP program RSEC_MIGRATION (transaction SA38 or SE38)
1. User Selection

Migration Step 1

- Choose users
  - Migration can be done for singular user groups

  ![Image](image.png)

  **Migration Authorizations: Set User**

  **Users for the Migration**

<table>
<thead>
<tr>
<th>User</th>
<th>Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERNARD</td>
<td></td>
</tr>
<tr>
<td>PETERA</td>
<td></td>
</tr>
<tr>
<td>LOA</td>
<td></td>
</tr>
</tbody>
</table>

  - Prerequisite: A user group must be complete and self-contained!

  If User 1 is chosen and Authorization Objects 1 and 2 should be migrated, you have to choose User 2 as well in order to have a complete user group.

Note: There might be entangled dependencies of users with respect to the authorization objects. You'll get a message with information on the missing users in case the user group is not complete.
Migration Step 2

Choose authorization objects to be migrated

<table>
<thead>
<tr>
<th>Reporting Authorization Obj. for Migration</th>
<th>Migrate</th>
<th>Authorization Object</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>YAUTHGEN</td>
</tr>
<tr>
<td></td>
<td>☑️</td>
<td>YRAC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>YRAD1</td>
</tr>
<tr>
<td></td>
<td>☑️</td>
<td>YRAH1</td>
</tr>
<tr>
<td></td>
<td>☑️</td>
<td>YRAM1</td>
</tr>
<tr>
<td></td>
<td>☑️</td>
<td>YRAN01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ZOOHIER</td>
</tr>
<tr>
<td></td>
<td>☑️</td>
<td>ZDIV00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ZMB_AUTH</td>
</tr>
<tr>
<td></td>
<td>☑️</td>
<td>ZTR_AUTH_PF</td>
</tr>
<tr>
<td></td>
<td>☑️</td>
<td>ZTR_COMP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S_RS_ICUBE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S_RS_ODSO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S_RS_ISET</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S_RS_MPRO</td>
</tr>
</tbody>
</table>
3. Assignment Method

Migration Step 3

■ Choose an assignment method

◆ Direct user assignment
  - Migrated authorizations will be assigned to the users directly (not via roles)
  - Migrated authorizations have prefix RSR_ and will be treated like generated authorizations

◆ Create new profiles
  - Generation of profiles based on authorization object S_RS_AUTH that contains the new, migrated authorizations
  - Preserves the existing role concept and adds new profiles to the role
  - Generated profiles have prefix RSR_

◆ Extend existing profiles
  - Existing profiles will be extended by authorization object S_RS_AUTH containing the migrated authorizations

◆ Undo migration
  - All migrated authorizations and profiles will be deleted; extended profiles contain empty authorization object R_RS_AUTH

Migration Authorizations: Characteristics

Select Assignment Method
- Direct Assignment to Users
- Generate New Profile
- Enhance Existing Profile
- Undo Migration
4. Migration Mode

Migration Step 4

- Choose details of authorization migration “expert mode”
  - Settings for referencing navigational attributes and characteristics are only relevant for the compatibility mode setting in SAP BW 3.x
  - Please have a look at the detailed documentation for more information

Details of Migration: Characteristics

- Execute Directly
- Execute in Background

Which Characteristics Receive Copies of Authorizations?

- [ ] Navigation Attributes (A..B)
- [ ] Referencing Navigation Attributes (A..BR)

- [ ] Navigation Attributes (A..B)
- [ ] Referencing Navigation Attributes (A..BR)
- [ ] Referencing Characteristic (BRH)
After the Migration Run

Migration Protocol

- At the end of the migration run, view the detailed protocol
- Check for warnings and errors reported during the migration

Tip: The migration can be quite tricky. It helps if you have good documentation of the existing authorization setup (for example, to define user groups for the migration)
<table>
<thead>
<tr>
<th>Overview of New Authorization Concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparison of Old and New Authorization Concepts</td>
</tr>
<tr>
<td>Authorization Maintenance</td>
</tr>
<tr>
<td>Generating Authorizations Automatically</td>
</tr>
<tr>
<td>Assigning Authorizations to Users and Roles</td>
</tr>
<tr>
<td>Monitoring, Auditing, and Test Tools</td>
</tr>
<tr>
<td>Migration</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
</tr>
</tbody>
</table>
Where to Find Free Public Technical Information

SAP Developer Network (it's free and public)
Where to Find Application and Educational Information

SAP Service Marketplace/security

Secure Business with SAP

Without Security, Business Simply Cannot Prosper

Data security at transaction level is a prerequisite to competing in the Internet economy. SAP offers best-in-class, comprehensive security solutions that protect data and ensure the confidentiality of business transactions. As a global solution provider and trusted advisor, SAP provides security technologies to protect the data processed by the mySAP Business Suite. The security infrastructure of SAP NetWeaver delivers comprehensive security features for heterogeneous environments. Combined with specialized partner solutions, its suite of state-of-the-art technology makes mySAP Business Suite the secure place to do business. For information on specific security-related topics, see Security in Detail.

News:
- Tutorial: How to create your own Java Custom Login Module (August 2004)
  If you need to secure an application you develop, you can do this using your own login module. This login module allows you to perform authentication in a different way than those provided with the JSSE Engine. By the end of this tutorial, you will be able to:
  - Use the SAP NetWeaver Studio to develop your own login module.
  - Deploy the login module to the JSSE engine.
  - Configure the login module on the JSSE engine.
- The SAP Security Newsletter for September 2004 is now available
  Hot off the press, you can find the new SAP NetWeaver Security Guide in the SAP Help Portal, or in the SAP Service Marketplace.
  This guide provides an introduction to security with the SAP NetWeaver platform as well as individual security guides for each of the SAP NetWeaver components.
  SAP now offers a specialist security certification for consultants. Available to anyone with a background in technical consulting, security certification provides proof to customers of a consultant’s knowledge in this area, as well as his or her ability to apply this knowledge practically in projects.
  You can find more information soon at SAP Consultant Certification. Use the booking code C-TAMPER-04 to register for certification.
  You can also find previous issues of the SAP Security newsletter in the security newsletter archive.

Spotlight:
- The SAP Security Solution Map is an outside-in approach, showing all the security aspects that companies require from their software. Under the individual topics, you can see whether SAP provides specific functionality or relies on partner products. You can take a look at the interactive map here, or download the print version.
  - Interactive SAP Security Solution Map
  - Print version SAP Security Solution Map (PDF, 264 KB)
SAP Security Web Information – Link Collection

http://sdn.sap.com*
http://service.sap.com/security*
http://service.sap.com/securityguide*
http://service.sap.com/education*
http://help.sap.com/nw2004s
mailto:security@sap.com

* Requires login credentials to the SAP Service Marketplace
The central hub for the SAP technology community

- Everyone can connect, contribute and collaborate- consultants, administrators and developers
- Focus around SAP NetWeaver and SAP xApps

High quality of technical resources

- Articles, how-to guides, weblogs, collaborative areas, discussion forums and downloads, toolkits and code-samples

A collaboration platform, not a one-way street

- SAP experts from customers, partners and SAP

SDN is powered by SAP NetWeaver™

- Built on the SAP Enterprise Portal
- Featuring collaboration capabilities of SAP Knowledge Management

Save Time and Effort
Analyzing Memory Problems in ABAP Programs with ABAP
Memory Inspector
10 Feb 2005

Diagnosing a memory problem in an ABAP application used to require analysis of expert-level system area displays in the ABAP debugger. Now there is a better way: The ABAP Memory Inspector. This article introduces the basics of memory management in the ABAP runtime environment, addresses common mistakes that can increase memory consumption, and demonstrates how the ABAP Memory Inspector can help you identify memory leaks in your programs by viewing dynamically created objects.
7 Key Points to Take Home

- BI authorizations for analysis are based on an appropriate concept for business-oriented security requirements.
- Using the new concept for analysis authorizations is recommended.
- The new features contain major improvements for administrators, leading to lower TCO.
- Authorizations can be generated automatically based on various DataStores.
- The infrastructure for maintenance and monitoring of analysis authorizations is highly integrated.
- Take a good look at the new reporting capabilities to support usage and auditing of authorizations.
- A migration support tool is available.
Questions?

Q&A

marc.bernard@sap.com