Internal Use SAP Partner Only

BW365

SAP BI - User Management & Authorizations

mySAP Business Intelligence

Date _____

Training Center _____

Instructors _____

_____

Education Website _____

Participant Handbook

Course Version: 2006 Q2
Course Duration: 2 Day(s)
Material Number: 50079390

An SAP course - use it to learn, reference it for work

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Copyright

Copyright © 2006 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Trademarks

- Microsoft®, WINDOWS®, NT®, EXCEL®, Word®, PowerPoint® and SQL Server® are registered trademarks of Microsoft Corporation.
- IBM®, DB2®, OS/2®, DB2/6000®, Parallel Sysplex®, MVS/ESA®, RS/6000®, AIX®, S/390®, AS/400®, OS/390®, and OS/400® are registered trademarks of IBM Corporation.
- ORACLE® is a registered trademark of ORACLE Corporation.
- INFORMIX®-OnLine for SAP and INFORMIX® Dynamic ServerTM are registered trademarks of Informix Software Incorporated.
- UNIX®, X/Open®, OSF/1®, and Motif® are registered trademarks of the Open Group.
- Citrix®, the Citrix logo, ICA®, Program Neighborhood®, MetaFrame®, WinFrame®, VideoFrame®, MultiWin® and other Citrix product names referenced herein are trademarks of Citrix Systems, Inc.
- HTML, DHTML, XML, XHTML are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.
- JAVA® is a registered trademark of Sun Microsystems, Inc.
- JAVASCRIPT® is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.
- SAP, SAP Logo, R/2, RIVA, R/3, SAP ArchiveLink, SAP Business Workflow, WebFlow, SAP EarlyWatch, BAPI, SAPPHIRE, Management Cockpit, mySAP.com Logo and mySAP.com are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other products mentioned are trademarks or registered trademarks of their respective companies.

Disclaimer

THESE MATERIALS ARE PROVIDED BY SAP ON AN "AS IS" BASIS, AND SAP EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR APPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THESE MATERIALS AND THE SERVICE, INFORMATION, TEXT, GRAPHICS, LINKS, OR ANY OTHER MATERIALS AND PRODUCTS CONTAINED HEREIN. IN NO EVENT SHALL SAP BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES OF ANY KIND WHATSOEVER, INCLUDING WITHOUT LIMITATION LOST REVENUES OR LOST PROFITS, WHICH MAY RESULT FROM THE USE OF THESE MATERIALS OR INCLUDED SOFTWARE COMPONENTS.

Internal Use SAP Partner Only

g20071225923

About This Handbook

This handbook is intended to complement the instructor-led presentation of this course, and serve as a source of reference. It is not suitable for self-study.

Typographic Conventions

American English is the standard used in this handbook. The following typographic conventions are also used.

Type Style	Description
Example text	Words or characters that appear on the screen. These include field names, screen titles, pushbuttons as well as menu names, paths, and options. Also used for cross-references to other documentation both internal (in this documentation) and external (in other locations, such as SAPNet).
Example text	Emphasized words or phrases in body text, titles of graphics, and tables
EXAMPLE TEXT	Names of elements in the system. These include report names, program names, transaction codes, table names, and individual key words of a programming language, when surrounded by body text, for example SELECT and INCLUDE.
`Example text`	Screen output. This includes file and directory names and their paths, messages, names of variables and parameters, and passages of the source text of a program.
`Example text`	Exact user entry. These are words and characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Pointed brackets indicate that you replace these words and characters with appropriate entries.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Icons in Body Text

The following icons are used in this handbook.

Icon	Meaning
	For more information, tips, or background
	Note or further explanation of previous point
	Exception or caution
	Procedures
	Indicates that the item is displayed in the instructor's presentation.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Contents

Course Overview ..... **vii**

Course Goals vii
Course Objectives vii

Unit 1: BI Overview **1**

BI Architecture and Administration 2
Business Explorer 11

Unit 2: Security Components in BI **23**

Comparison of OLTP and OLAP Security Needs 24
Authorizations in BI 30

Unit 3: Securing Data Access for Reporting Users **43**

Analysis Authorization 45
Securing Data Access for Reporting Users 52
How to Use BI-Specific Authorization Values 73
Defining Security Using Hierarchies 86
Monitoring Analysis Authorizations (Trace Functions) 97
Important Aspects of BI Authorizations 108
Tracing Authorizations 114

Unit 4: Saving BEx Objects to BI Roles **131**

Securing Workbooks 132

Unit 5: Securing Data Access for Administration Users **155**

Securing Data Access for Administrators 156
System Communication Security 173

Unit 6: Maintaining Authorizations **187**

Maintaining Authorizations 188
Using Templates 204
Migrating Authorizations 210

Unit 7: Authorizations for Business Planning and Simulation **221**

Planning in BI 222

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Interaction Between Planning and Other BI Activities 227

Unit 8: Appendices 235

Performance Measurement and Recommendation 236
Structural Authorizations BI/mySAP ERP HCM 241

Glossary 249

Index 257

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Course Overview

This course is about the security concept in SAP BI. The focus is the specific security elements of SAP BI.

Target Audience

This course is intended for the following audiences:

- Those responsible for setting up and managing authorizations for BI.

Course Prerequisites

Required Knowledge

- BW305 or BW310 or equivalent BI experience

Recommended Knowledge

- ADM940
- Previous SAP security experience in R/3 or mySAP ERP.

Course Goals

This course will prepare you to:

- Describe how security is implemented in SAP NetWeaver BI.
- Implement and manage security in an BI environment.

Course Objectives

After completing this course, you will be able to:

- Describe BI architecture and how it relates to your security policies.
- Explain the differences and similarities between mySAP ERP security requirements and BI security requirements.
- Secure reporting users, including the authorization objects and authorization values required.
- List the types of tasks required by administration users and describe how to secure those tasks.

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

- Describe the Business Content roles and templates provided by SAP to assist you in building security for your BI system.
- Explain the security required for systems providing data to BI.

SAP Software Component Information

The information in this course pertains to the following SAP Software Components and releases:

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Unit 1

BI Overview

Unit Overview

This unit reviews the essential information needed for BI security administrators. The information presented in this unit is also contained in the prerequisite courses BW305 and BW310.

Unit Objectives

After completing this unit, you will be able to:

- Describe the major components of the BI architecture
- Describe the flow of data into BI
- List the major functions of the Data Warehousing Workbench
- Describe the Business Explorer and list the major components
- Explain the link between SAP BI and Microsoft Excel
- Create a simple query from an existing InfoCube
- Execute a query and then launch it on the web.

Unit Contents

Lesson: BI Architecture and Administration 2
Lesson: Business Explorer 11
Exercise 1: ICreate and Execute a BI Query 15

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: BI Architecture and Administration

Lesson Overview

This lesson will present an overview of the architecture of SAP Netweaver 2004s BI and briefly discuss the administration tools available to manage the flow of data into BI.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the major components of the BI architecture
- Describe the flow of data into BI
- List the major functions of the Data Warehousing Workbench

Business Example

As a security administrator for your company, you have been asked to analyze the BI system and recommend a suitable strategy for securing access to both BI and the data within. You need a good understanding of both the architecture of BI and the tools used to manage data in the system.

The Architecture of BI

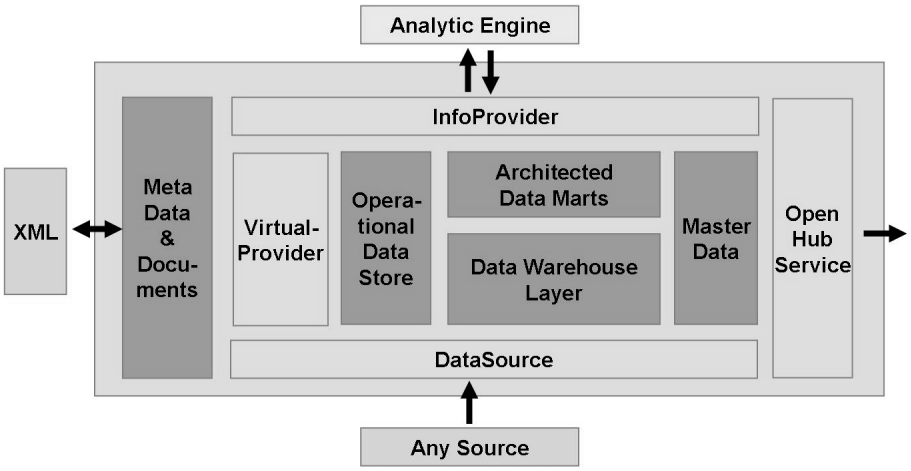


Figure 1: BI Architecture

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

BI has a multilevel architecture to provide the maximum degree of flexibility. BI can extract and use data from a variety of sources. These include all mySAP Business suite components (mySAP ERP, CRM, PLM, SCM, SRM, R/3, APO); non-SAP systems; flat files; XML files; web services; commercial data providers; and even other BI systems. The BI server provides all the tools necessary to model, extract, transform, aggregate, store, and access data. Since the description of the data, regardless of its source, is contained in a common metadata repository, data from a variety of sources can be combined to give you enhanced data analysis options. BI users can access data through the Business Explorer suite, Enterprise Portal, Information Broadcasting, any standard Web browser, or certified third-party reporting tools.

Extracting, Transforming and Loading Data

In many companies, data is fragmented and spread across many databases and applications. Decision makers need information to develop a comprehensive view of the company and to answer key business questions accurately and completely. To be useful, data must be integrated, standardized, synchronized and enriched. This is done through a process known as extraction, transformation, and loading (ETL).

The data must be collected and cleansed to eliminate duplicate and incorrect values. Then the data must be enhanced to transform it into practical, clear information for the company.

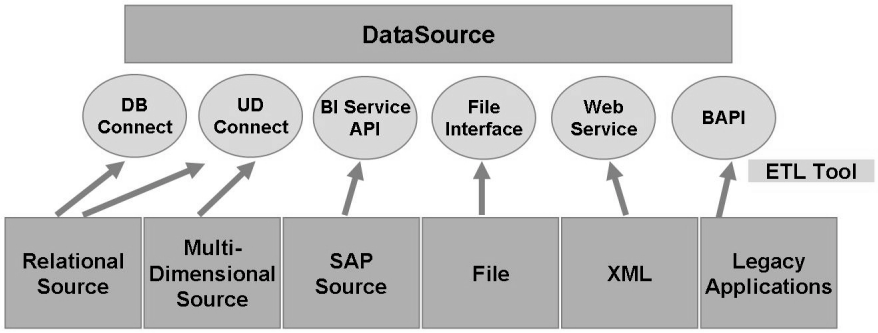


Figure 2: Broad ETL Capabilities

BI provides a broad set of ETL capabilities that supports data extraction at the application and file levels. Data can be loaded from virtually any source, as shown above. In the figure, data is made available to BI according to the source data definitions in each of the DataSources.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Information Model

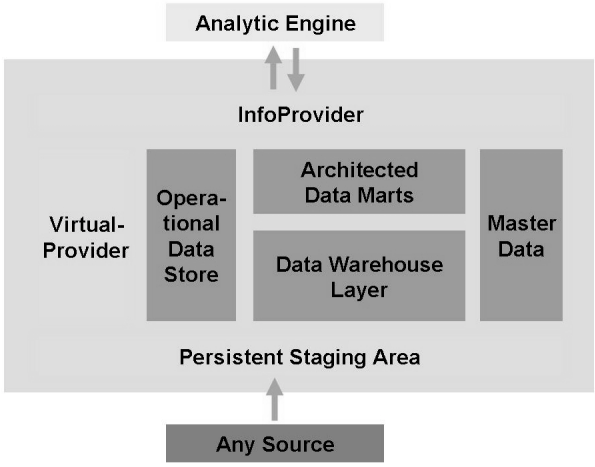


Figure 3: Information Model - Conceptual Layers

The key conceptual layers in the BI information model are:

Persistent Staging Area (PSA)

In the BI information model, data is physically stored in the PSA object, a transparent database table. A PSA object is the initial storage area of data, where requested data is saved, unchanged from the source system, according to the structure defined in the DataSource. A PSA can be created for each DataSource and source system.

Data Warehouse

The result of the first transformations is saved in the next layer, the data warehouse. This data warehouse layer offers integrated, granular, historic, stable data. This layer provides the basis for building consistent reporting structures and allows you to react to new requirements with flexibility.

Architected Data Marts

Architected Data Marts are multidimensional reporting structures. This layer satisfies reporting requirements. The term “architected“ refers to the fact that these data marts are not isolated applications but are based on a universally consistent data model.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Operational Data Store

In addition to analytical and strategic reporting, a data warehouse also supports operative reporting by means of the operational data store. Data can be updated to an operational data store on a continual basis or at short intervals and is available for operational reporting. Operational data can also be forwarded to the data warehouse layer at set times.

The BI information model is based on a fundamental building block called the **InfoObject.** InfoObjects are business evaluation objects such as customer or sales. InfoObjects are subdivided into characteristics, key figures, time characteristics or units, and are easily reused. An InfoObject has three classes of metadata: technical (data type, length), business definition (such as key performance indicators) and user metadata which carries information about authorizations. All components of the information model store metadata.

Hint: From a security perspective, InfoObjects are similar to fields in mySAP ERP.Securing access by company code in mySAP ERP would be analogous to securing access by the InfoObject for company code in BI.

Data Acquisition

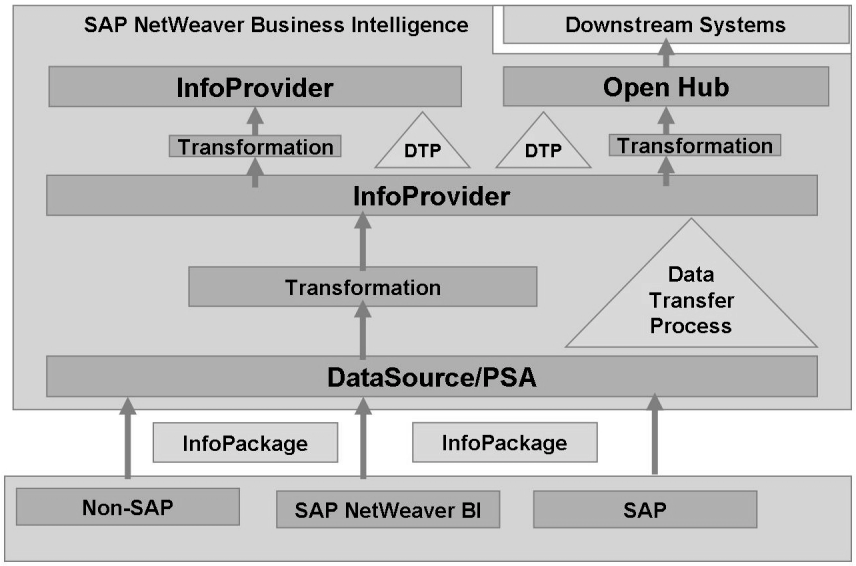


Figure 4: Data Flow in BI

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Data can be loaded from the Persistent Staging Area directly into the operational data store and the data warehouse. It can also be loaded directly into multidimensional InfoCubes if there is no need to consolidate and keep the data in the operational data store or data warehouse sections.

Data is transferred to BI with InfoPackages. An InfoPackage dictates what data defined in a DataSource should be requested from a source system. An InfoPackage can request both transaction and master data. To do this, it uses precise parameters, such as "only controlling area 0001 in timeframe 10/2005". InfoPackages can also describe specific subsets of data in the DataSource. The Data Warehousing Workbench schedules and monitors the transfer of InfoPackages.

The data transfer process (DTP) transfers data from a persistent object to another object following certain transformation rules. Data transfer processes are used for standard data transfer, for real-time data acquisition, and for accessing data directly.

The open hub service allows you to distribute data from a BI system to non-SAP data marts, analytical applications, and other applications. It allows you to ensure controlled distribution across several systems. With the open hub service, the BI system is the hub of an enterprise data warehouse. The distribution of data is transparent by scheduling and central monitoring of the distribution status in the BI system. BI objects such as InfoCubes, DataStore objects, or InfoObjects (attributes or texts) can function as open hub data sources.

Information Access

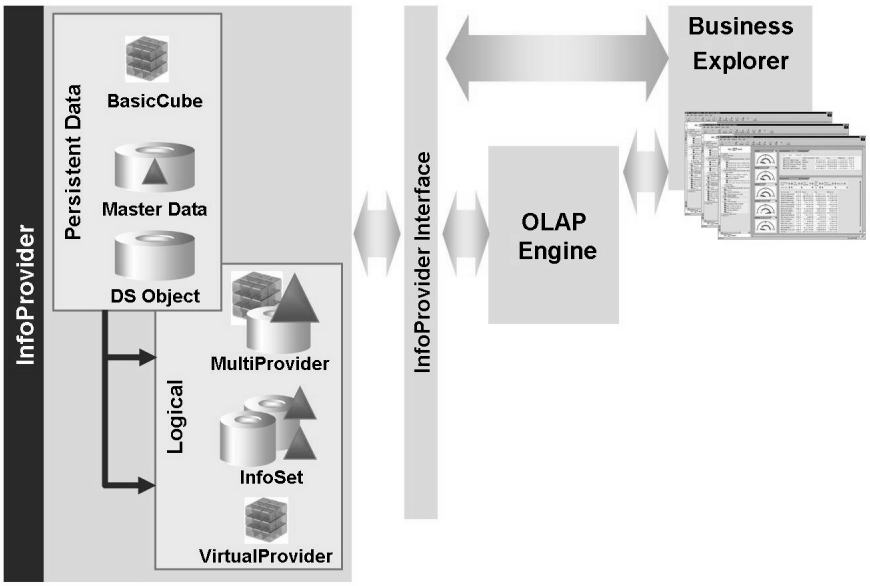


Figure 5: InfoProviders and Analysis Tools

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

In BI, objects that provide information for reporting and analysis are called InfoProviders. There are two types of InfoProviders: physical and logical. InfoObjects, InfoCubes, and Data Store Objects contain physical data. InfoSets, RemoteCubes, and MultiProviders are logical structures and do not contain data.

An InfoCube is a transaction data container. In an InfoCube, data is organized in terms of business dimensions. When reporting from an InfoCube, users can perform multidimensional analysis from different business perspectives. For example, sales analysis could be performed across different geographic regions or distribution channels.

MultiProviders are used to combine data from various objects. A MultiProvider provides access to data from several InfoProviders and makes the data available for reporting and analysis. A MultiProvider can be assembled from different combinations of InfoProviders.

Users can access BI information with several different tools. The Business Explorer Suite is provided as an integral part of BI. Users may also access BI information through a Web browser, or Enterprise Portal, providing an easy-to-implement interface. Certified third-party tools are also available.

Data Warehousing Administration

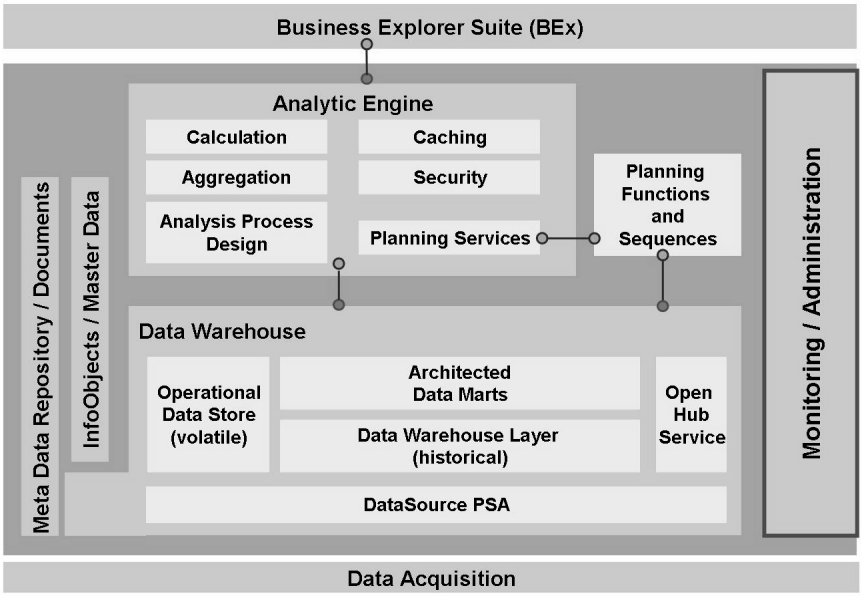


Figure 6: BI Architecture: Monitoring

© 2006 SAP AG. All rights reserved.

Modeling and running an enterprise data warehouse is highly complex and requires the support of adequate tools. Administrators must manage the data warehousing processes to ensure that information is current and continues to provide the data that decision makers need. Administrators must respond to changes quickly, so that the company can identify and take advantage of fast-moving opportunities.

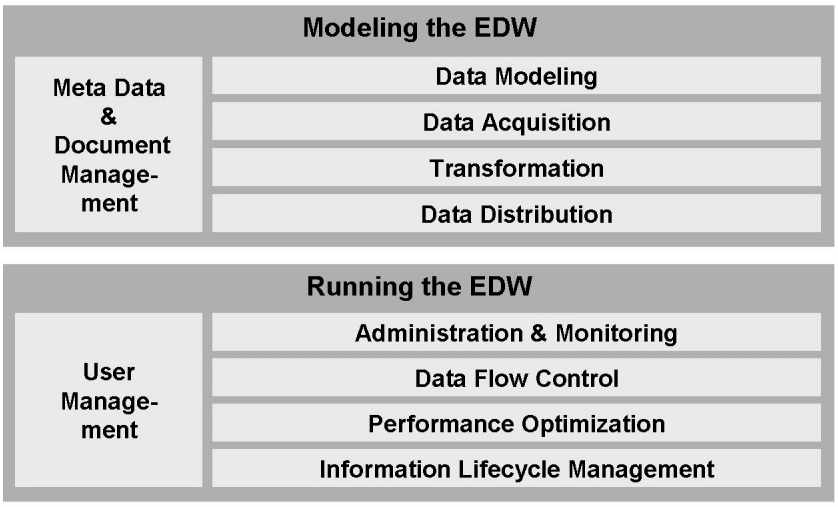


Figure 7: Modeling and Running the Enterprise Data Warehouse

To enable administrators to meet these changing needs, BI provides a single, central environment for data warehouse management: the **Data Warehousing Workbench**. The Data Warehousing Workbench provides the tools needed to support modeling and running the data warehouse.

In the Data Warehousing Workbench, modeling functions provide access to InfoProviders, InfoObjects, InfoSources and DataSources.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Data Warehousing Workbench

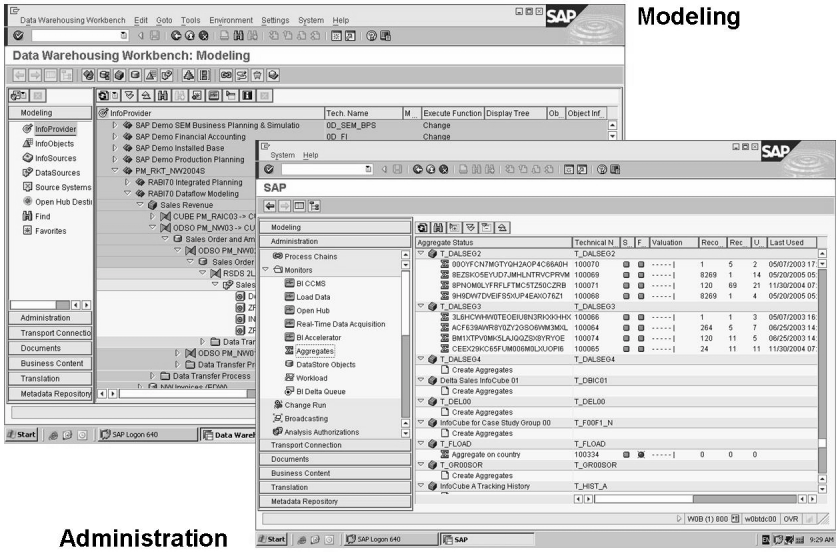


Figure 8: Data Warehousing Workbench

Administration tools needed to run the data warehouse, such as monitoring extractions and workload analysis, are summarized in another area of the Data Warehousing Workbench.

Authorization

To ensure that your data warehousing solution reflects your company's structure and business needs, it is critical that you establish who is authorized to access what data. With BI, authorizations can be defined and maintained by object: InfoObject, query, InfoProviders and hierarchies. Authorizations can be inserted into roles that are used to determine what type of content is available to specific users or user groups. Role templates and Business Content Roles are delivered with BI.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Describe the major components of the BI architecture
- Describe the flow of data into BI
- List the major functions of the Data Warehousing Workbench

Related Information

- For more information about the SAP Business Information Warehouse, visit the BI page at http://service.sap.com/BI.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Business Explorer

Lesson Overview

In this lesson, you will gain an overview of the Business Explorer, its components, and their functions. You will see how Microsoft Excel functions as a user interface for the display of queries and how queries can be displayed using a Web browser. You will create a simple query and execute it.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the Business Explorer and list the major components
- Explain the link between SAP BI and Microsoft Excel
- Create a simple query from an existing InfoCube
- Execute a query and then launch it on the web.

Business Example

Your company wants to use BI for its reporting needs. You wish to gain an overview of how the Business Explorer facilitates the creation, maintenance, and organization of queries.

Components of the Business Explorer Suite

The Business Explorer is the standard business intelligence tool delivered with BI. It includes several components, each designed to perform a specific task to enable many forms of analysis.

The tools in the Business Explorer (BEx) Suite, allow business experts to create and distribute the necessary reports and analyses. These tools are integrated with each other and have user-friendly, intuitive interfaces.

Detailed analysis of BI information can be done both on the Web and in Microsoft Excel with BEx tools. BI information can be accessed using the Enterprise Portal. With information broadcasting functions customers are able to distribute BI information by e-mail, or broadcast it to Knowledge Management (KM folders) and collaboration rooms in the Enterprise Portal.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

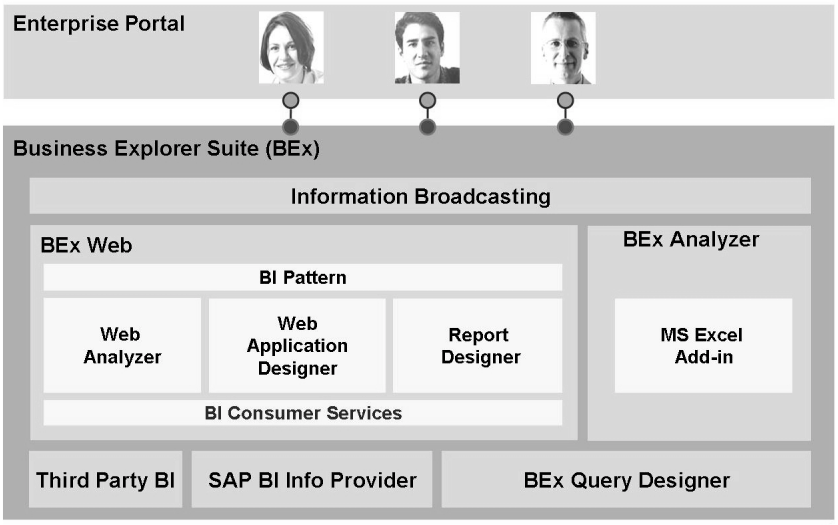


Figure 9: Business Explorer Suite

The Web Application Designer is the tool that used to create Web applications. The Report Designer is used to create formatted reports. The Web Analyzer is used for Web-based ad hoc analysis.

The Query Designer is the BEx Tool used to create BI queries.

It is flexible and user-oriented.

Characteristics and Key Figures are added to queries using Drag and Drop.

Additional functions are available using context menus.

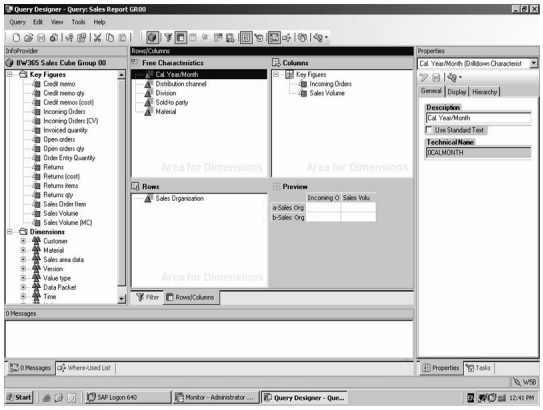


Figure 10: Business Explorer: Query Designer

The Query Designer is the BEx tool used to create BI queries. It is a very flexible and user-oriented tool. To create queries, users select characteristics and key figures from the global lists on the left side of the screen and drag and drop the selections to the proper area on the right side of the screen. InfoObjects can be placed in Rows or Columns. Another section for Free characteristics is provided. From the context

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

menus of the InfoObjects, additional options are available to support query design. For example, users can restrict values or affect the display properties of objects from the context menus.

Query output can be displayed in Table or Graphic format.

Flexible and intuitive navigational functions are available.

Reports can be viewed using MSEXCEL or on the WEB.

Information Broadcasting can distribute reports :

- to email addresses.
- Knowledge Management folders, Collaboration Rooms on Enterprise Portal.

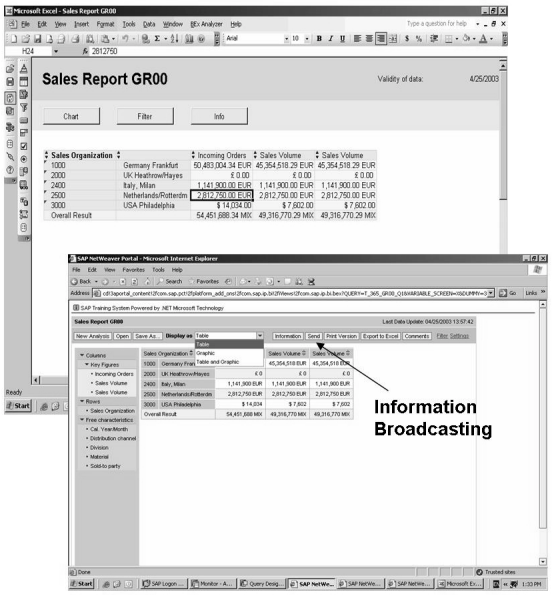


Figure 11: BI Query Execution

The query results may be displayed in tabular or graphic format. Flexible and intuitive navigational functions are available from the context menus. All queries can be viewed from the MS Excel environment or on the Web. Web queries can be executed from a URL or from within a Web Application.

The Information Broadcasting function allows query results to be distributed using email addresses. Query results may also be distributed to folders in the Knowledge Management environment in the Enterprise Portal or to Collaboration Rooms in the Enterprise Portal.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Exercise 1: ICreate and Execute a BI Query

Exercise Objectives

After completing this exercise, you will be able to:

- Create a simple query from an existing InfoCube, execute it, and save it as a new workbook

Business Example

You wish to create a simple query to display order and invoice volume by customer and material.

Task:

As user BW365-##, create a new query for incoming order value and sales volume by customer and material from your Sales Infocube, **T_365SD##** . Give the query a descriptive name of **Invoice Report GR##** and a technical name of **GR##BW365Q1** and save it to your *Favorites* folder. Execute the query. Launch the query on the web.

Note: Change Log on language if your web templates appear in the wrong language

1. Logon to the BEx Analyzer and find your InfoCube, T_365SD##
2. Create your new query**,INVOICE REPORT GR##,** using the Query Designer. Execute your query and launch it on the web.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Solution 1: ICreate and Execute a BI Query

Task:

As user BW365-##, create a new query for incoming order value and sales volume by customer and material from your Sales Infocube, **T_365SD##** . Give the query a descriptive name of **Invoice Report GR##** and a technical name of **GR##BW365Q1** and save it to your *Favorites* folder. Execute the query. Launch the query on the web.

Note: Change Log on language if your web templates appear in the wrong language

1. Logon to the BEx Analyzer and find your InfoCube, T_365SD##
   a) As user BW365-##, where ## represents your assigned group number, follow *START → Programs→Business Explorer → Analyzer*.
   b) Select *Tools → Create New Query* from the BEx toolbar.
   c) From the Query Designer toolbar choose *New Query*.
   d) Choose *InfoAreas*.
   e) Select *BW Training → BW Customer Training → BW365 Authorization → Group ## → BW365 Sales Cube Group ##.*

Continued on next page

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

2. Create your new query **,INVOICE REPORT GR##,** using the Query Designer. Execute your query and launch it on the web.

   a) Double-click on your InfoCube, *BW365 Sales Cube Group ##.*

   b) You will now be on the *Query Designer: New Query* screen. The left column of the screen contains all of the objects in your InfoCube that are available for use in the query definition.On the bottom of the screen choose *Rows/Columns.*

   c) On the left, open the *Key Figure* section. Drag *Incoming orders* to the *Columns* window of the screen. Notice that a node called *Key Figures* is created automatically.

   d) Drag key figure *Sales Volume* to the *Columns* window and drop it underneath *Incoming Orders*.

   e) Expand the *Customer* dimension. Drag *Sold-to Party* to the *Rows* window.

   f) Expand the *Material* dimension and drag *Material* to the *Free Characteristics* window.

   g) Choose *Save Query*.

   h) In the *Description* field, enter **INVOICE REPORT GR##**. In the *Technical Name* field, enter **GR##BW365Q1** and choose *Save*.

   i) Choose *Quit and Use Query* to view the query results.

   j) Choose *Tools, BEx Web Analyzer* to launch your report on the web.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Describe the Business Explorer and list the major components
- Explain the link between SAP BI and Microsoft Excel
- Create a simple query from an existing InfoCube
- Execute a query and then launch it on the web.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Unit Summary

You should now be able to:

- Describe the major components of the BI architecture
- Describe the flow of data into BI
- List the major functions of the Data Warehousing Workbench
- Describe the Business Explorer and list the major components
- Explain the link between SAP BI and Microsoft Excel
- Create a simple query from an existing InfoCube
- Execute a query and then launch it on the web.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Test Your Knowledge

1. The DataSource is a collection of related InfoObjects for the purpose of extracting data, and is defined in BI.

   Determine whether this statement is true or false.

   - □ True
   - □ False

2. The Data Warehousing Workbench is used to maintain the objects that build the data warehouse, such as InfoCubes and InfoObjects.

   Determine whether this statement is true or false.

   - □ True
   - □ False

3. Which of the following is NOT created or maintained using the tools of the Data Warehousing Workbench?

   Choose the correct answer(s).

   - □ A InfoAreas
   - □ B InfoCubes
   - □ C Queries
   - □ D InfoObjects
   - □ E InfoSources
   - □ F Source Systems

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Answers

1. The DataSource is a collection of related InfoObjects for the purpose of extracting data, and is defined in BI.

   Answer: False

   The DataSource is a collection of field names representing data that can be extracted from a source system. A collection of related InfoObjects for data extraction in BI is called an InfoSource.

2. The Data Warehousing Workbench is used to maintain the objects that build the data warehouse, such as InfoCubes and InfoObjects.

   Answer: True

   The Data Warehousing Workbench is the toolset used most often by BI administrators to carry out their work.

3. Which of the following is NOT created or maintained using the tools of the Data Warehousing Workbench?

   Answer: C

   Queries are created and maintained using the Query Designer.

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Unit 2

Security Components in BI

Unit Overview

The topic of this unit is security requirements for BI and mySAP ERP in generaI. Not only does it compare the role of security functions in BI implementation with the role of security functions in an mySAP ERP implementation, it also compares the security requirements of OLAP (Online Analytical Processing) and OLTP (Online Transaction Processing).

This unit also introduces the authorization concept in BI.

Unit Objectives

After completing this unit, you will be able to:

- Describe security needs in an OLTP environment
- Describe security needs in an OLAP environment
- Explain the differences in security approaches for OLTP versus OLAP
- Describe how authorization objects are used for security.
- Describe BI authorization objects and what the BI authorization objects protect.
- Explain when BI authorization object should be used.

Unit Contents

Lesson: Comparison of OLTP and OLAP Security Needs 24
Lesson: Authorizations in BI 30
Exercise 2: Review Authorization Objects in BI 35

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson: Comparison of OLTP and OLAP Security Needs

Lesson Overview

This lesson will discuss the differences in security needs between an OLAP (SAP NetWeaver BI) system and an OLTP (mySAP™ ERP) system. It will focus on the differences in business strategy, and how security must be approached from a different perspective.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe security needs in an OLTP environment
- Describe security needs in an OLAP environment
- Explain the differences in security approaches for OLTP versus OLAP

Business Example

How you implement security for a user in mySAP ERP may be different than how you implement security for the same user in BI. It is important to understand the difference in what the user is trying to achieve in a BI system and how security must meet those differing needs.

Security Needs in mySAP™ ERP (OLTP)

When you designed security for your mySAP ERP system you were driven by transaction codes and field values. There are many transaction codes in mySAP ERP, and you have to make sure that certain users can only get to certain transaction codes. Many of you set up mySAP ERP security at a very detailed level. Additionally, you also had to set up security for each user, which could number in the thousands. In general, mySAP ERP security is focused on:

- Transaction codes
- Specific field values
- Which activities a user can perform

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

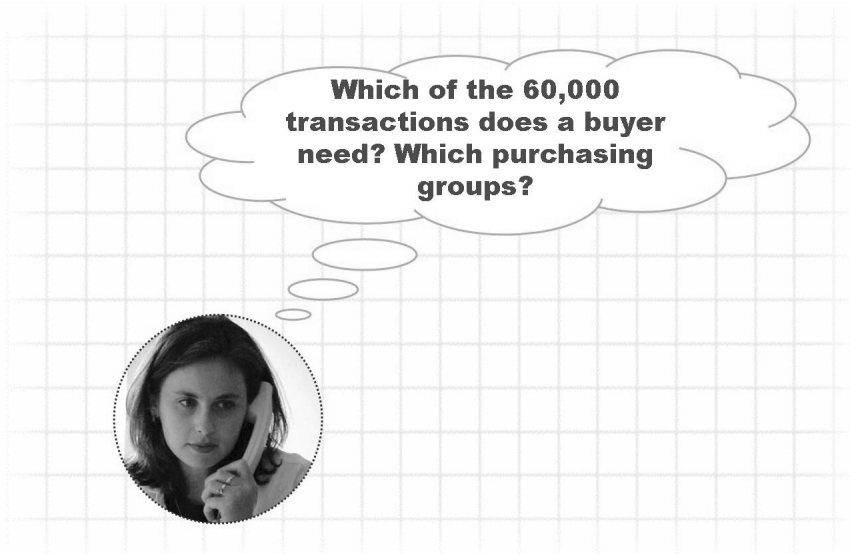


Figure 12: Transaction-Based Security

mySAP ERP is an OLTP (online transaction processing) system. This means that mySAP ERP focuses on getting the daily work of the business completed as quickly and efficiently as possible. People only need access to the specific functions they perform in this daily work.

Security Needs in BI (OLAP)

The security requirements of a BI system are different from those of an mySAP ERP system. A BI system has a very different business purpose and business goals from an mySAP ERP system. It is important to understand the difference. Security must be approached differently if the BI implementation is to be successful.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Figure 13: Analysis-Based Security

Activities in BI

There is no creation of purchase orders, sales orders, or material master records in BI. There is no updating of business data in BI. The primary activities in BI are displaying data and analyzing results. The end users will only be analyzing data, not updating it.

Security Focus in BI

The security function in BI does not put the focus on transaction codes or activities. Instead it focuses on the data itself. The security function in BI focuses on:

- InfoAreas
- InfoProvider (InfoCube, DataStore Objects)
- Queries

BI is focused on what data a user can access. This may be controlled at the field level, or it may be controlled at the InfoProvider level. The InfoProvider is a category of objects that can provide data to a query, such as InfoCubes and DataStore Objects. The InfoCube or DataStore Object holds the summarized data that the user can then analyze. Query results are based on the data in the InfoProvider.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

OLTP versus OLAP

Characteristics	OLTP	OLAP
Primary operation	Update process	Analyze
Level of analysis	Low	High
Amount of data per transaction	Very small	Very large
Type of data	Detailed	Summary
Timeliness of data	Must be current	Current and historical
Updates to data	Frequently	Less frequent, new data only
Database design	Complex	Simple
Number of transactions/users	Many (100s to 1000s)	Few
Response time	Quick	Reasonable
Database data	Normalized	Denormalized
No. of tables per transaction	Several	Few
Type of processing	Well-defined	Ad hoc

Arrow indicates a strong effect on security

Figure 14: Contrast Security Needs in mySAP ERP Versus BI

In BI, the primary operation is analysis work. The user analyzes the summarized data in an InfoCube. The data is not updated by the end user. The user accesses all the data in the InfoProvider by using a reporting tool like the BEx Analyzer.

Security Strategy in BI Versus mySAP ERP

In mySAP ERP, security is focused around detailed information in purchasing groups, company codes, cost centers, plants, or business areas. Your company may have a few key fields that are an integral part of your security strategy.

If you secure BI exactly the same as you secure mySAP ERP, then you might be hindering the value you company can gain from BI. In BI, if a user executes a query and only receives results from company code 1000, then they can only make business decisions based on that one company code. In order to discover important trends, they may need to see data from all company codes.

When a user executes a query, they will receive only the results they are authorized to see. For example, if a manager only has access to company code 1000, after execution of the query, only data for company code 1000 is output. In order to make the best decision, the manager may need results from company codes 1000, 2000 and 3000,

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

even if this is only available in aggregated form. It is critical that you discuss security with the BI team and try to first establish the goals of an BI system and how those goals will impact security.

If you need to secure down to the company code level, or any other level (sales organization, division, business area, etc); you can in BI. Before implementing security, you need to ensure the level of security is in line with the goals of the BI implementation.

Figure 15: Manager Using BI

BI is not about creating and updating data, it is about converting data into knowledge. Security is an integral part of an BI implementation, and must be considered when establishing the goals of your BI implementation.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Lesson Summary

You should now be able to:

- Describe security needs in an OLTP environment
- Describe security needs in an OLAP environment
- Explain the differences in security approaches for OLTP versus OLAP

© 2006 SAP AG. All rights reserved.

Lesson: Authorizations in BI

Lesson Overview

This lesson introduces authorizations in BI. There are two major types of authorizations in BI. One type focuses on Administrative users and another type focuses on Reporting users. Authorizations for Administrative users in many ways parallel mySAP ERP security, but securing BI reporting users is much different.

Because the security concept for Reporting users is much more complicated, a different concept and special tools are required. This unit introduces the concept of Analysis Authorizations.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe how authorization objects are used for security.
- Describe BI authorization objects and what the BI authorization objects protect.
- Explain when BI authorization object should be used.

Business Example

Your BI implementation project requires that you secure your users by application area. You need to understand what authorization objects are provided by BI to enable you to meet that goal.

Authorization Objects in BI

Authorization objects enable you to define complex authorizations by grouping up to 10 authorization fields in an AND relationship to check whether a user is allowed to perform a certain action. To pass an authorization test for an object, the user must satisfy the authorization check for each field in the object.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

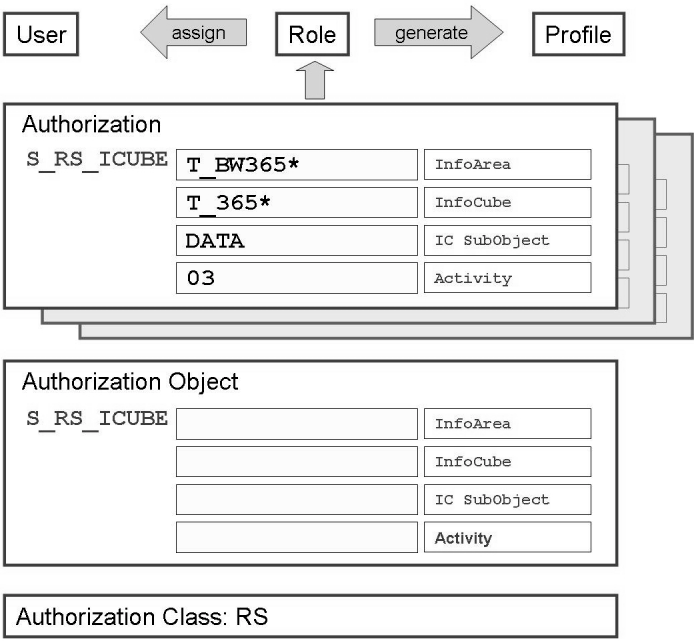


Figure 16: Authorzation Objects

Authorization objects are grouped according to authorization object classes. The major authorization object class in BI is RS.

Authorization Objects in Object Class RS.

Transaction SU21.

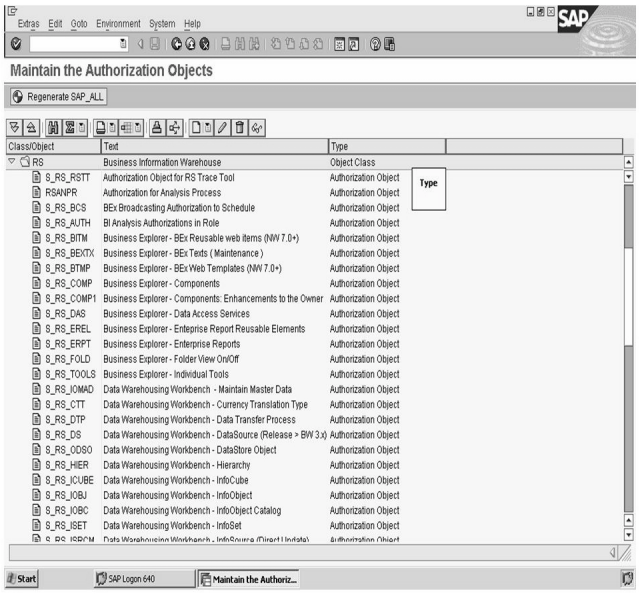


Figure 17: Authorization Objects in Object Class RS

© 2006 SAP AG. All rights reserved.

There are some authorization objects in authorization object class RS that are used primarily for Reporting users. There are other authorization objects in this class that are used primarily for Administrator users.

Authorization Objects Used Primarily by Reporting Users

In order to execute any query, you must have access to S_RS_COMP, a powerful authorization object that enables you to make choices on how to secure. There is one field in S_RS_COMP that relates to the query, and another field that relates to the InfoCube. This gives you the option to secure by query name, InfoArea, or InfoCube.

Hint:

- InfoArea = group of InfoCubes
- InfoCube = actual data
- InfoObject = field (for example: company code, plant, or cost center)

The following table describes the authorization objects used to secure a reporting environment.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

BI Authorization Objects Used In Reporting

Technical Name	Description	Example
S_RS_COMP	Authorizations for using different components for the query definition. This authorization object is very important for reporting.	Your company has decided that each power user can create queries only for their application area. You are using a naming convention for each area. S_RS_COMP can be used to enforce this policy (for example, in accounts receivables all queries must start with AR). **OR** Your company has decided that each power user can create queries only for their application area. You have linked the application area to a specific InfoArea and InfoCube. The power user can create any query with any name as long as they only create queries for "their" InfoCube. S_RS_COMP can also be used to enforce this policy. The first example ties to the query name, the second example ties to the InfoCube.

Authorization Objects Used Primarily by Administrators

BI administrators have a large range of tasks they must complete: setting up InfoCubes, managing the loading of data from the source systems, managing the Data Transfer Process and handling all the transformations. Many Administrator tasks are secured with the authorization object S_RS_ADMWB.

The authorization objects that are specifically designed for administrative tasks are discussed in much more in a later unit.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Exercise 2: Review Authorization Objects in BI

Exercise Objectives

After completing this exercise, you will be able to:

- Describe authorization objects provided in BI and explain how they are used

Business Example

You need to understand what authorization objects are unique to BI, when to use the objects, and what they protect.

Task:

In this exercise you will look at the online help for some of the BI authorization objects. You will explore when and why the authorization objects are used.

1. Find the documentation for the authorization object S_RS_COMP. Use the documentation to answer the next two questions.

2. Fields in S_RS_COMP can protect the query elements by InfoArea, InfoCube, and query name that a user is trying to access.
   Determine whether this statement is true or false.
   □ True
   □ False

3. In the BEx Analyzer, where can you see the InfoArea, InfoCube, and query?

   _____
   _____
   _____
   _____

4. Find the documentation for the authorization object S_RS_ADMWB. Use the documentation to answer the next two questions.

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

5. S_RS_ADMWB is only used by reporting users.
   Determine whether this statement is true or false.
   - □ True
   - □ False

6. Which of the statements below accurately describe when S_RS_ADMWB will be used?
   Choose the correct answer(s).
   - □ A When using transaction code RSA1, the DataWarehousing Workbench
   - □ B When creating a new query in the BEx Analyzer
   - □ C When updating source systems in RSA1
   - □ D When creating a new sales order

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Solution 2: Review Authorization Objects in BI

Task:

In this exercise you will look at the online help for some of the BI authorization objects. You will explore when and why the authorization objects are used.

1. Find the documentation for the authorization object S_RS_COMP. Use the documentation to answer the next two questions.

   a) *Tools → Administration → User Maintenance → Authorizations and Profiles (Manual Maintenance) → Edit Authorizations Manually* (transaction code SU03).

   b) Double click on the class "RS" which has the description *Buisness Information Warehouse* (clicking on the text does not work)

   c) Click once on the object **S_RS_COMP** and choose *Documentation*.

2. Fields in S_RS_COMP can protect the query elements by InfoArea, InfoCube, and query name that a user is trying to access.

   Answer: True

   The major fields in the S_RS_COMP object are for protecting the InfoArea, InfoProvider, and component type. An InfoCube is an example of an InfoProvider and a query is one of the component types. There are also fields for activity and for the aspect of the query you are protecting.

3. In the BEx Analyzer, where can you see the InfoArea, InfoCube, and query?

   Answer: In BI, execute transaction code RRMX to bring up the BEx Analyzer. On the SAP BW toolbar, choose *Open → Queries*. Choose *InfoAreas*. Then choose *Technical Name On/Off*. As you drill down, you can see the InfoAreas, InfoCubes, and queries, each with their own icon. The query is the lowest branch of the tree structure. S_RS_COMP protects what the user can execute.

4. Find the documentation for the authorization object S_RS_ADMWB. Use the documentation to answer the next two questions.

   a) *Tools → Administration → User Maintenance → Authorizations and Profiles (Manual Maintenance)→ Edit Authorizations Manually* (transaction code SU03).

   b) Double-click on the object class *Business Information Warehouse*.

   c) Click once on the object **S_RS_ADMWB** and choose *Documentation*.

Continued on next page

 © 2006 SAP AG. All rights reserved.

5. S_RS_ADMWB is only used by reporting users.

   Answer: False

   S_RS_ADMWB is used for administrative tasks in BI.

6. Which of the statements below accurately describe when S_RS_ADMWB will be used?

   Answer: A, C

   Answers A and C are correct because they both involve administration tasks.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Describe how authorization objects are used for security.
- Describe BI authorization objects and what the BI authorization objects protect.
- Explain when BI authorization object should be used.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Unit Summary

You should now be able to:

- Describe security needs in an OLTP environment
- Describe security needs in an OLAP environment
- Explain the differences in security approaches for OLTP versus OLAP
- Describe how authorization objects are used for security.
- Describe BI authorization objects and what the BI authorization objects protect.
- Explain when BI authorization object should be used.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Test Your Knowledge

1. Which of the following best describes the security needs in an mySAP ERP OLTP environment?
   Choose the correct answer(s).
   - □ A Driven by the transaction code
   - □ B Driven by activities: create, change display
   - □ C Driven by analysis tools
   - □ D Driven by field values: company code, sales organization, purchasing groups

2. Your BI security strategy should parallel your mySAP ERP security strategy.
   Determine whether this statement is true or false.
   - □ True
   - □ False

3. The primary authorization objects in BI include:
   Choose the correct answer(s).
   - □ A S_RS_ADMI
   - □ B S_RS_COMP
   - □ C S_RS_ADMWB
   - □ D S_RS_PLOG

4. Authorization object S_RS_HIER is used when creating InfoCubes.
   Determine whether this statement is true or false.
   - □ True
   - □ False

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Answers

1. Which of the following best describes the security needs in an mySAP ERP OLTP environment?

   Answer: A, B, D

   An OLTP environment is focused on who can perform specific actions on specific fields. The transaction code is the first thing checked.

2. Your BI security strategy should parallel your mySAP ERP security strategy.

   Answer: False

   Before you decide what strategy to use, you must talk with the BI team to discuss the goals of you BI system. Some control elements in BI are possibly similar to control elements in mySAP ERP. However, it is also possible that the BI system uses other control elements to enable business decisions based on a wider data basis.

3. The primary authorization objects in BI include:

   Answer: B, C

   Authorization object S_RS_COMP protects queries; S_RS_ADMWB protects RSA1.

4. Authorization object S_RS_HIER is used when creating InfoCubes.

   Answer: False

   Authorization object S_RS_HIER is related to hierarchies. It primarily protects who can create hierarchies and who can execute queries that use hierarchies.

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Unit 3

Securing Data Access for Reporting Users

Unit Overview

This unit will explain how to implement user security reporting in a BI environment. It discusses the both the options that exist and the steps required for securing reporting users.

Unit Objectives

After completing this unit, you will be able to:

- Define the purpose of Analysis Authorizations.
- Describe how to create an Analysis Authorization.
- Describe how to incorporate an Analysis Authorization into a role./
- Explain the options available for securing data access for reporting users.
- List the steps required for InfoObject-level security.
- Define security by InfoArea, InfoCube, and InfoObject.
- Limit security by query owner.
- List authorization values that are specific to BI
- Define security for aggregated values
- Explain how to use variables in regards to authorizations
- Explain how hierarchies are used in BI.
- Explain why security is necessary for hierarchies.
- Demonstrate how to secure hierarchies.
- Describe the purpose of the analysis authorization trace
- Use the trace function
- Explain how to read the trace results
- Understand the most important aspects of BI authorizations on an overview level.
- Avoid common misunderstandings with BI authorizations.

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

- Explain the purpose of the ST01 trace in regards to authorizations
- List the differences between ST01 and the trace for analysis authorizations

Unit Contents

Lesson: Analysis Authorization 45
Lesson: Securing Data Access for Reporting Users 52
Procedure: Steps to Implement InfoObject Security (Field-Level Security) 56
Exercise 3: Set up InfoObject-Level Security for Reporting Users..... 59
Exercise 4: Using S_RS_COMP1 and S_RS_FOLD 67
Lesson: How to Use BI-Specific Authorization Values 73
Exercise 5: Using BI-Specific Authorization Values..... 79
Lesson: Defining Security Using Hierarchies 86
Procedure: Maintaining Authorizations for Hierarchies..... 89
Exercise 6: Query Authorizations for Securing Hierarchies..... 91
Lesson: Monitoring Analysis Authorizations (Trace Functions)..... 97
Exercise 7: Tracing BI Authorizations 105
Lesson: Important Aspects of BI Authorizations 108
Lesson: Tracing Authorizations 114
Exercise 8: ST01 Trace.....117

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Lesson: Analysis Authorization

Lesson Overview

This lesson introduces Analysis Authorizations.

Lesson Objectives

After completing this lesson, you will be able to:

- Define the purpose of Analysis Authorizations.
- Describe how to create an Analysis Authorization.
- Describe how to incorporate an Analysis Authorization into a role./

Business Example

You need to provide security to protect reporting users.

Analysis Authorizations

- **On InfoCube level**
- **On characteristic level**
- **On characteristic value level**
- **On key figure level**
- **On hierarchy node level**

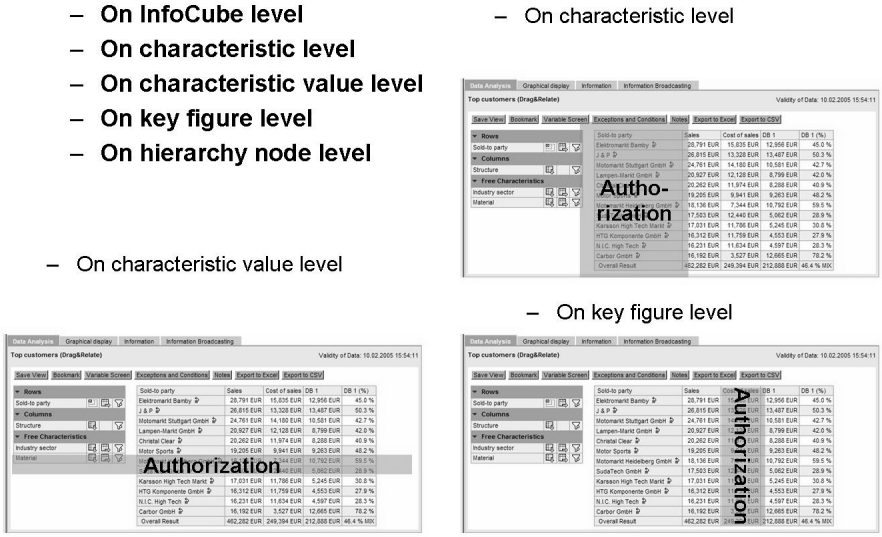


Figure 18: Authorization Levels for BI Reporting

If you restrict users to a certain InfoCube then this may be an easy way to set up and maintain authorizations but this will severely restrict access. This would mean users can either access ALL the data in an InfoCube or NO data in the InfoCube.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

For securing reporting users, you may want to define authorizations at a much lower level than the InfoCube.

The options include :

- InfoCube Level: Restrict at the InfoCube level.
- Characteristic Level: Restrict access to all values for a particular characteristic.
- Characteristic Value Level: Restrict access to certain values of a particular characteristic.
- Key Figure Level: Restrict access to certain key figures.
- Hierarchy Node: Restrict access to certain nodes of a hierarchy.

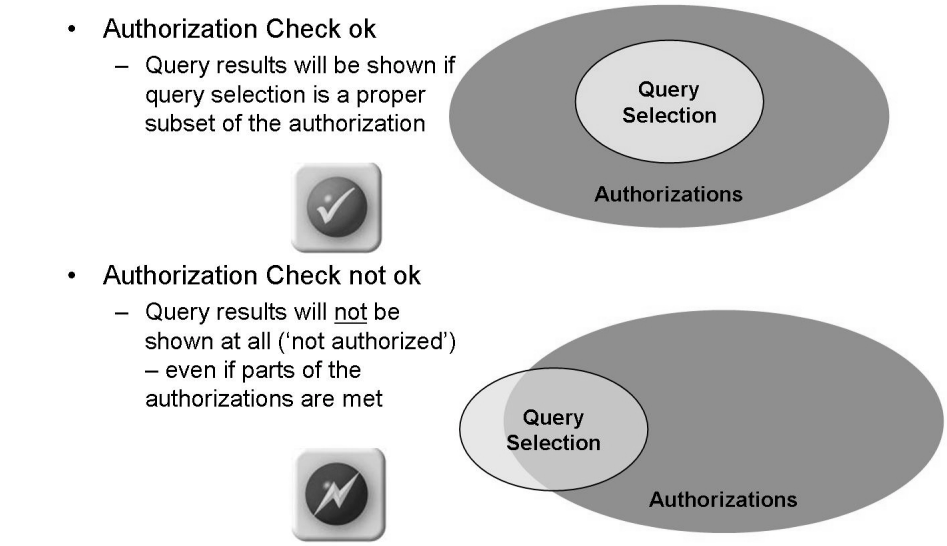


Figure 19: Authorization Checks in BI Queries

You either get the compete result or nothing at all.

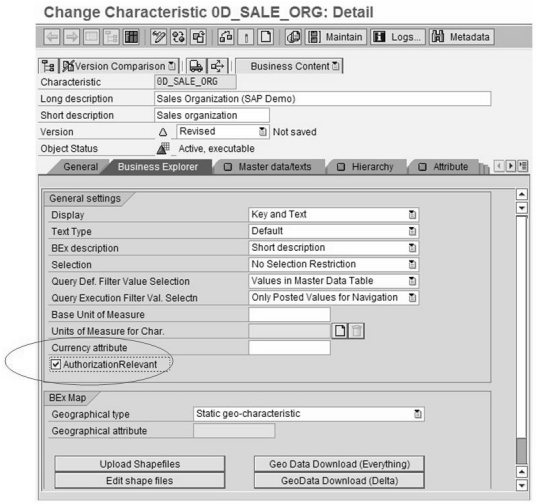
Exceptions to this rule:

- Display hierarchies are automatically filtered by the authorization (the system doesn't give you a blank result just because you should only see a part of the hierarchy. You will see only the nodes you are authorized to see.
- Key figure values are not displayed if the key figure is not authorized. You don't get a blank screen if you don't have access to one or two key figures – you will still see the key figures you are authorized to see.

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Characteristics must be flagged as *Authorization Relevant* before they can be secured.

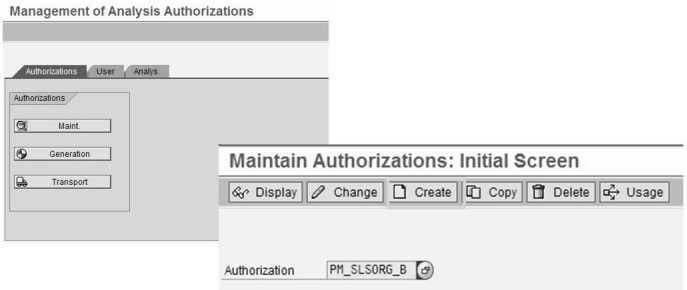


InfoObject maintenance / transaction RSD1

Figure 20: Authorization Relevant Characteristics

InfoObjects must be flagged as *Authorization Relevant* before they can be secured.

RSECADMIN



A group of users is authorized only to specific sales organizations.

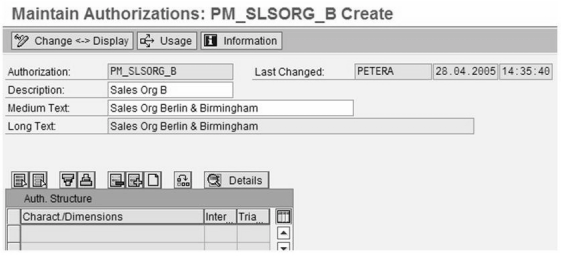


Figure 21: Analysis Authorizations Central Maintenance: RSECADMIN

Prerequisites : You have authorization for authorization object S_RSEC.

The first step to create an analysis authorization is to choose the characteristics which you want to secure. You can choose multiple characteristics.

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

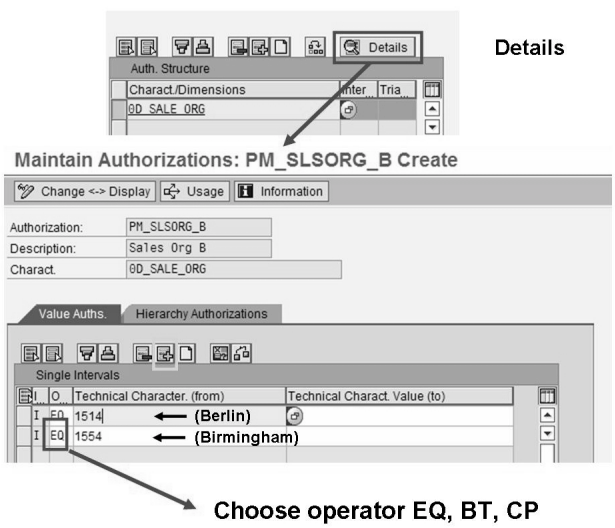


Figure 22: Analysis Authorization: Values

Next choose the values for the characteristics you have defined in the previous step. You can choose:

- EQ : single value
- BT: range of values
- CP : contain pattern, e.g ABC*

Required Business Content Characteristics

Three Business Content characteristics are required:

- Activity (0TCAACTVT): e.g. reading (03)
- InfoProvider (0TCAIPROV): grants authorization to particular InfoProviders
- Validity (0TCAVALID): grants authorization to specific time periods

They must be assigned to a user in at least one authorization.
They must not be included in queries!

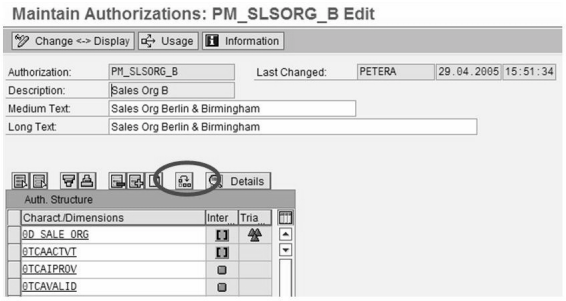


Figure 23: Required Business Content Characteristics

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

There are 3 special Business Content characteristics which SAP recommends that you include in at least one of your authorizations:

- **0TCAACTVT**, Activity: display (03), etc.
- **0TCAIPROV**, InfoProvider: grants authorization to particular InfoProviders.
- **0TCAVALID,** Validity: grants authorization to specific time periods.

Required Business Content Characteristics

Three Business Content characteristics are required:

- Activity (0TCAACTVT): e.g. reading (03)
- InfoProvider (0TCAIPROV): grants authorization to particular InfoProviders
- Validity (0TCAVALID): grants authorization to specific time periods

They must be assigned to a user in at least one authorization.
They must not be included in queries!

RSECADMIN

Insert special characteristics.

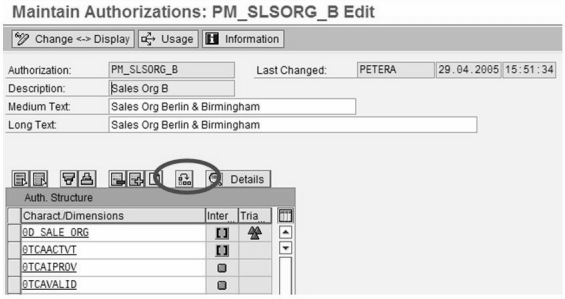


Figure 24: Required Business Content Characteristics

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 using authorization object S_RS_AUTH.

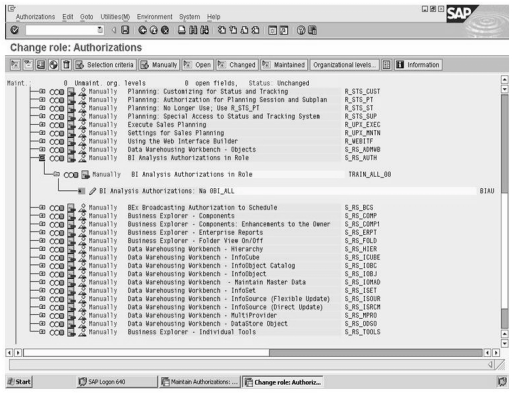


Figure 25: Special Authorization: 0BI_ALL

© 2006 SAP AG. All rights reserved.

An authorization for all values of all authorization-relevant characteristics is created automatically in the system. It has the name **0BI_ALL.** It can be viewed, but not changed. Every user that receives this authorization can access all the data at any time. Each time an InfoObject is activated and the property authorization relevant is changed for the characteristic or a navigation attribute, 0BI_ALL is automatically adjusted.

A user that has a profile with the authorization object S_RS_AUTH and has entered 0BI_ALL (or has included it, for example with the pattern *) has complete access to all data.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Define the purpose of Analysis Authorizations.
- Describe how to create an Analysis Authorization.
- Describe how to incorporate an Analysis Authorization into a role./

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Securing Data Access for Reporting Users

Lesson Overview

This lesson will discuss both the minimum authorizations needed by reporting users and how to secure reporting users down to the InfoObject level.

Lesson Objectives

After completing this lesson, you will be able to:

- Explain the options available for securing data access for reporting users.
- List the steps required for InfoObject-level security.
- Define security by InfoArea, InfoCube, and InfoObject.
- Limit security by query owner.

Business Example

You have restricted access for reporting users by InfoCube. A sales manager can run any query created for InfoCube T_365SD##. However, each sales manager is responsible for a specific division. Although all sales managers can run the same query, the results should be displayed only for their assigned division. You need to enable a reporting user to query data by their assigned division.

Note: Please remember as we walk through this lesson that you may or may not need to implement security as detailed as BI allows. For example, if you are trying to make global decisions about how sales are performing, then you need to see data for all regions. Users are making business decisions based on query results. Data that is too limited could result in decisions that do not meet the overall strategic goals of your business.

Minimum Authorization Requirements for a Reporting User

- Analysis authorizations for an InfoProvider
- S_RS_COMP (Activities 03, 16)
- S_RS_COMP1 (Query owner)
- S_RFC (BEx Analyzer or BEx Browser only)
- S_TCODE (RRMX for BEx Analyzer)

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

A reporting user must have authorizations for the S_RS_COMP, S_RS_COMP1 authorization objects as well as analysis authorizations for the InfoProvider on which the query is based.

In addition, if the reporting user will be using the BEx Analyzer reporting tool, they will need authorizations for object S_RFC and S_TCODE with authorization for transaction code RRMX.

Options for Securing Data Access for Reporting Users

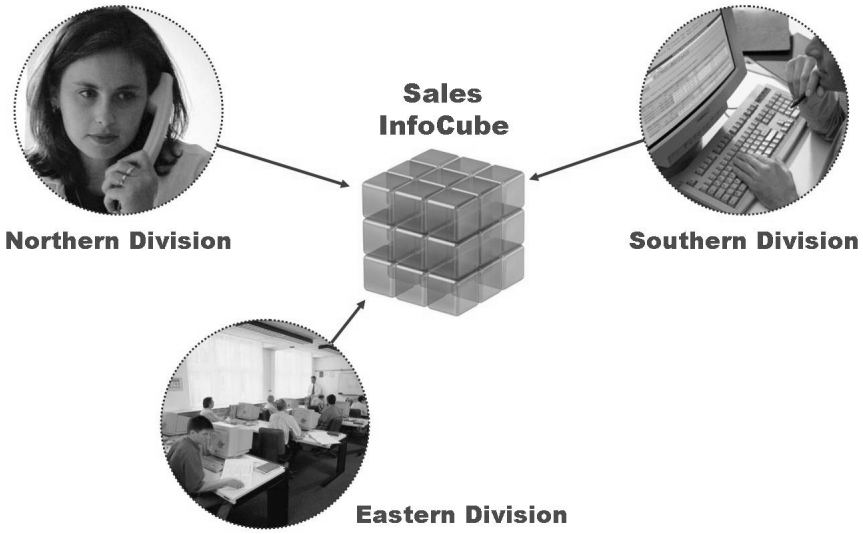


Figure 26: Secure by InfoCube

One option for securing reporting users is to divide users into groups. This would work, for example, if the authorizations need to be checked only on InfoProvider level. You can then create roles that allow you to run queries from the specified InfoProvider(s).

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

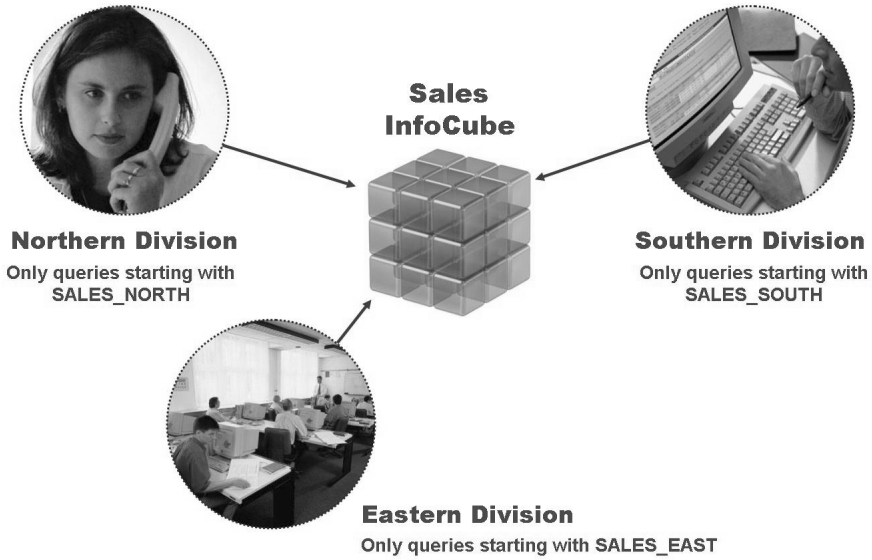


Figure 27: Securing by Query

Another option would be to use the InfoProvider in conjunction with the query name. To do this, you will need a strict naming convention for query names so that security does not have to be updated each time a new query is created.

However, neither of the options above meet the requirements of our business scenario. If you want two users to execute the same query, but to get different results based on their assigned division, cost center, or some other InfoObject, then you must secure down to the InfoObject level. This option is the closest parallel to the field-level security that is normally done in traditional mySAP ERP.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

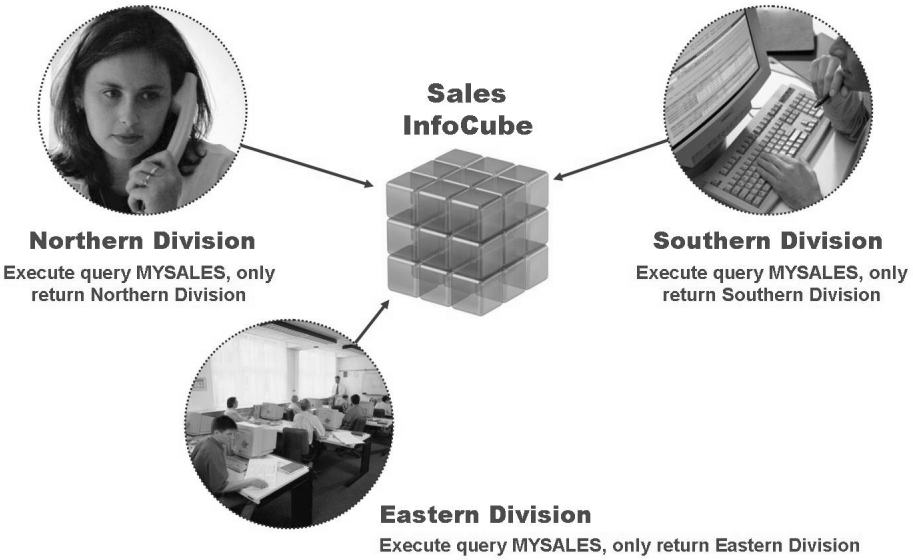


Figure 28: Securing by InfoObject

If you secure purchase orders by purchasing group, sales orders by sales organization, or financial data by cost center, then you may need to implement field-level security in BI. Security on the field level is achieved in BI by restricting access up to the level of the InfoObjects, since InfoObjects correspond to the fields in mySAP ERP. In our business example, the data should be protected that is displayed independent of the division.

Setting Up Security for an InfoObject

In our business scenario, we need to secure by the InfoObject 0DIVISION. Currently we can only secure down to the InfoCube level. When a sales manager executes a query, the results should be different based on their assigned division.

The following procedure shows the steps you must following when setting up security for an InfoObject:

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Steps to Implement InfoObject Security (Field-Level Security)

1. Define the InfoObject as authorization relevant.

   The *Authorization Relevant* setting for an InfoObject made in the InfoObject definition on the *Business Explorer* tab. The business needs will drive which InfoObjects should be relevant for security. Keep in mind that the people using BI are running queries to help make strategic decisions on how to better run the business. The decision makers typically need to see more data on BI than they would need to see in mySAP ERP.

2. Create (or adjust) analysis authorizations for the InfoObject.

   So far no analysis authorizations exist for the InfoObject. You can create new authorizations or adjust existing ones to include the InfoObject and corresponding authorized values. This is done In transaction RSECADMIN. Only InfoObjects that have been marked *Authorization Relevant* are eligible to be put in an analysis authorization.

3. Assign authorizations to users.

   Once you have created analysis authorizations, users will need access to the right authorizations according to business needs. You can assign authorizations in roles using S_RS_AUTH or directly in transaction RSECADMIN or RSU01.

4. Add a variable to the queries.

   The reason the variable is required is sometimes unclear at first. If we want a query to only provide results based on the division, for example, then the query itself needs the ability to filter specific division values. Before we can secure on division, the query must be able to restrict data by division. The only way the query can restrict data dynamically is through a variable. The variable can be added anytime independent of the other steps listed here.

Additional Options for Reporting Users

- S_RS_COMP1: Secure by query owner.
- S_RS_FOLD: Disable the *InfoAreas* button in the BEx Analyzer *Open Queries* dialog box.

In addition to securing down to the InfoObject level, you may also want to secure by query owner. This would be the case if sales managers can execute queries by division and there is a power user for each division creating the queries needed. For example,

 © 2006 SAP AG. All rights reserved.

for the High Tech division, Frank is the power user. That would mean that any sales manager for the High Tech division could only execute queries created by Frank. Authorization object S_RS_COMP1 is the object that enables protection in this way.

When a user brings up the BEx Analyzer or uses the Query Designer for Web-based reporting, there are four categories from which they may choose existing queries: *History*, *Favorites*, *Roles*, and *InfoAreas*. Authorization object S_RS_FOLD will allow you to disable the *InfoAreas* category.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Exercise 3: Set up InfoObject-Level Security for Reporting Users

Exercise Objectives

After completing this exercise, you will be able to:

- Defining InfoObject-Level Security for Reporting Users

Business Example

In your company, you wish to restrict the data that reporting users see to only their assigned division. Currently all users can report on data for all divisions. You need to secure queries so that each reporting user can only access data in their division. In this exercise, your Reporting user should only have access to data for division 01.

Task 1:

Create the user **REPORTING-##** by copying REPORTING-99. You will then have 2 userids: **BW365-##** (Administrator) and **REPORTING-##** (Reporting user). Log on with the Administrator user, **BW365-##,** and analyze the query **T_365_GR##_Q1.** Review all the data for all divisions.

1. Create the user **REPORTING-##** by copying REPORTING-99. Specify an initial password of your choice for the new user ID. Take note of the role that was assigned to your new user.
2. Log on to the BEx Analyzer as **BW365-##**. Execute the query with the technical name of **T_365_GR##_Q1**. In the query result, drill down by division. Notice that you have access to data for several divisions.

Task 2:

Ensure that InfoObject T_DIV_365 is marked as authorization-relevant.

1. Find the technical name for the *Division* InfoObject used in the previous step.
2. Verify that InfoObject T_DIV_365 is marked as authorization relevant (do this as your Administrator user, BW365-##).

Hint: From InfoObject Maintenance, search for the InfoObject T_DIV_365 and verify that this InfoObject is already **authorization relevant**.

Continued on next page

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Task 3:

Create your own custom Analysis Authorization to protect the *Division* field. Assign your Reporting-## user to this new Analysis Authorization.

1. As user BW365-##, create your own Analysis Authorization, **ZDIV##**. This object should include the InfoObject T_DIV_365. Assign your Reporting-## user to this new Analysis Authorization. Include the Special Characteristics: 0TCAACTVT, 0TCAIPROV and 0TCAVALID.
2. Assign your Reporting-## user to your new Analysis Authorization, ZDIV##. By assigning your Reporting-## user to your new Analysis Authorization, that user will only have access to Division 01 (Pumps).

Task 4:

Update the query to add a variable to the BW365 Division InfoObject. Only your Administrator user, **BW365-##** has the authorization to change a query definition. After you have made the change to your query, execute the query as your Reporting-## user. This user should only be able to see Division 01, Pumps when drilling down by division in the query/

1. As your Administrator user, **BW365-##**, log on to the BEx Analyzer and add a Characteristic variable for Division to your Sales Report query (T_365_GR##_Q1).
2. As your Reporting-## user, execute your Sales Report query, T_365_GR00_Q1. When prompted, select Pumps for the variable prompt. When the query displays, drill down on Division. You should only see Divison 01, Pumps.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Solution 3: Set up InfoObject-Level Security for Reporting Users

Task 1:

Create the user **REPORTING-##** by copying REPORTING-99. You will then have 2 userids: **BW365-##** (Administrator) and **REPORTING-##** (Reporting user). Log on with the Administrator user, **BW365-##,** and analyze the query **T_365_GR##_Q1.** Review all the data for all divisions.

1. Create the user **REPORTING-##** by copying REPORTING-99. Specify an initial password of your choice for the new user ID. Take note of the role that was assigned to your new user.

   a) *Tools → Administration → User Maintenance → Users*.

   b) Enter **`REPORTING-99`** in the *User* field. Choose *Copy*.

   c) Enter **`REPORTING-##`** as the *To* user. Accept the default settings in the *Choose parts* section of the screen. Choose *Copy*.

   d) Enter an initial password of your choice. Select the *Roles* tab to look at the roles and see this user has the role **REPORTING_BASIC** assigned to them.

   e) Save the new user master record by choosing *Save*.

Continued on next page

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

2. Log on to the BEx Analyzer as **BW365-##**. Execute the query with the technical name of **T_365_GR##_Q1**. In the query result, drill down by division. Notice that you have access to data for several divisions.

   a) To log on to the BEx Analyzer as **BW365-##** , from the Windows *Start* menu, choose *Start → Programs → Business Explorer → Business Explorer →Analyzer*. You will be prompted for your userid and password when you attempt to open the list of available queries. Enter your Administrator userid and password.

   b) From the BEx toolbar, select *Open → Query* and choose *InfoAreas*.

   c) Expand the InfoAreas tree structure by following *BW Training → BW Customer Training → BW365 Authorization → Group ## → BW365 Sales Cube Group ## → Sales Report GR##.*

   d) Show the technical names of the objects by choosing the Wrench Icon ("Display Object Name as")

   e) Select the query and choose *open* .

   f) Once the query results appear, choose Filter. Double click on division. You will see the query drilldown, and you should see results for various divisions.

Task 2:

Ensure that InfoObject T_DIV_365 is marked as authorization-relevant.

1. Find the technical name for the *Division* InfoObject used in the previous step.

   a) In the previous exercise, you executed the query *T_365_GR##_Q1* as your Administrator user, BW365--##. From the BEx toolbar, select *Tools → Edit query.*

   b) When the query definition appears, turn on technical names by choosing *Technical Name* (wrench icon).

      Notice the technical name for the *Division* InfoObect. It should be T_DIV_365.

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

2. Verify that InfoObject T_DIV_365 is marked as authorization relevant (do this as your Administrator user, BW365-##).

Hint: From InfoObject Maintenance, search for the InfoObject T_DIV_365 and verify that this InfoObject is already **authorization relevant**.

a) From the SAP main menu, follow *Modeling → Object maintenance →InfoObject (RSD1)*.

b) Enter the InfoObject T_DIV_365 and press Display.

c) In the InfoObect definition, select the *Business Explorer* tab. Note that the *Authorization Relevant* checkbox is selected. If it is not selected, please inform your instructor. Do not change the setting yourself.

d) Return to the *SAP* menu.

Continued on next page

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Task 3:

Create your own custom Analysis Authorization to protect the *Division* field. Assign your Reporting-## user to this new Analysis Authorization.

1. As user BW365-##, create your own Analysis Authorization, **ZDIV##**. This object should include the InfoObject T_DIV_365. Assign your Reporting-## user to this new Analysis Authorization. Include the Special Characteristics: 0TCAACTVT, 0TCAIPROV and 0TCAVALID.

   a) As user BW365-##, follow the path *SAP menu → Business Explorer → Manage Analysis Authorizations*.

   b) From the Authorizations tab select **Maint.**

   c) In the *Authorization* field, enter **`ZDIV##`** and press *Create*.

   d) Enter short , medium and long text of **`Gr## Secure by Div.`**.

   e) Insert a row by pressing the + icon.

   f) Enter *T_DIV_365* and press enter.

   g) Highlight the row with *T_DIV_365* and choose Details.

   h) Insert a row by choosing the + icon.

   i) Select **I** in the *Including/Excluding* column.

   j) Select **EQ** in the *Operator* column.

   k) Enter **01** in the *Characteristics from* column.

   l) Save. Press green arrow back.

   m) Choose *Insert Special Character.* The Special Characteristics (0TCAACTVT, 0TCAIPROV and 0TCAVALID) should now be added to your Analysis Authorization

   n) Save. Return to Management of Analysis Authorizations. (Green arrow back. Green arrow back.)

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

2. Assign your Reporting-## user to your new Analysis Authorization, ZDIV##. By assigning your Reporting-## user to your new Analysis Authorization, that user will only have access to Division 01 (Pumps).
   a) Choose the *User* tab.
   b) Choose *Assign.*
   c) In the User field enter your **Reporting-##** user id and choose *Change.*
   d) In the Authorizations section enter the Name: **ZDIV##** and press Insert.
   e) Save. Return to the SAP menu. (Green arrow back. Green arrow back.)

Task 4:

Update the query to add a variable to the BW365 Division InfoObject. Only your Administrator user, **BW365-##** has the authorization to change a query definition. After you have made the change to your query, execute the query as your Reporting-## user. This user should only be able to see Division 01, Pumps when drilling down by division in the query/

1. As your Administrator user, **BW365-##**, log on to the BEx Analyzer and add a Characteristic variable for Division to your Sales Report query (T_365_GR##_Q1).
   a) From the Start menu select *Programs→ Business Explorer → Business Explorer→ Analyzer.*
   b) Using the *Open* dialog, select your query (*T_365_GR##_Q1*). The query is probably in your *History* listing. If so, just select it . If the query is not in your *History* section, then either enter the technical name, or follow the path *BW Training → BW Customer Training → BW365 Authorizations → Group ## → BW365 Sales Cube Group ## → Sales Report GR##.* Once you open the query, select it then choose *Tools → Edit Query* from the BEx toolbar.
   c) Expand the Sales Area Dimension. Expand the BW365 Division Characteristic. Expand the Characteristic Value Variables. You should see the variable T_DIV365. This is a Characteristic variable, with processing by manual input. When this variable is assigned to Division, there will be a prompt for Division when the query is executed.
   d) Press **Filter** at the bottom.
   e) From the context menu for Division, choose *Restrict.*
   f) In the Show window choose *Variables.*

Continued on next page

 © 2006 SAP AG. All rights reserved.

g) Highlight T_365DIV and copy it to the Selection list on the right by pressing the right arrow. Press *OK* and then press *Save*.

h) Return to the Bex Analyzer by pressing the *green check* icon (Exit and Use Query)

i) You should now have an input prompt for division. If you leave the division blank, your query result will display all divisions during drill down. If you select a specific division, only that division will display during drill down. Leave division blank. When the query results are displayed, choose FILTER and doube click on Division. You should see all division in the drilldown. (Divisions: 00, 01, 02, 04, 07, 08, 20)

2. As your Reporting-## user, execute your Sales Report query, T_365_GR00_Q1. When prompted, select Pumps for the variable prompt. When the query displays, drill down on Division. You should only see Divison 01, Pumps.

a) Logon as your Reporting-## user. *Start → Programs → Business Explorer → Business Explorer →Analyzer*. You will be prompted for your userid and password when you attempt to open the list of available queries. Enter your Reporting userid and password. If this is the first time you are logging on as your Reporting-## user you will be prompted to enter a new password after you enter the initial password.

b) Open the query T_365_GR00_Q1 by selecting *Open→ Query* from the BEx Toolbar.

To open it just type the exact technical name in the search window accessed by selecting the *Find* Icon

c) When prompted by the Division Characteristic variable, select **Pumps** from the drop down list of divisions. The technical name for Pumps is 01. In the custom Analysis Authorization you entered the technical name.

d) When the query results display, choose FILTER and then click on Division. You should see division included in the results, but only Pumps (division 01) should display. This is because your Reporting-## user only has access to division 01, based on the Analysis Authorization that you created.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Exercise 4: Using S_RS_COMP1 and S_RS_FOLD

Exercise Objectives

After completing this exercise, you will be able to:

- Limit query access within the BEx Analyzer

Business Example

You have power users who create queries. You want to give the sales manager for the northern region access to all queries created by the sales power user. The sales manager should not be able to see queries created by the HR power user.

Task 1:

Create your own role, called **REPORTING_BASIC_##**, by copying the REPORTING_BASIC role. In the new role, update the authorization for object S_RS_COMP1 to only see queries where BW365-## is the query owner.

1. As user BW365-##, copy role REPORTING_BASIC to a new role called **REPORTING_BASIC_##**. When prompted, choose *Copy Selectively* and accept all default values.
2. For your new role, **REPORTING_BASIC_##**, change the authorization information. On the *Authorizations* tab, update authorization object S_RS_COMP1 by changing the *Owner* field value from * to **BW365-##**.
3. Generate the role. Accept the default profile name.
4. Remove the role REPORTING_BASIC from the user REPORTING-## and give REPORTING-## your new role, **REPORTING_BASIC_##**. Do this by maintaining the user master record directly. When finished, REPORTING-## should only contain one role: REPORTING_BASIC_##.

Task 2:

Log on to the BEx Analyzer as REPORTING-## and note which queries the user can access.

1. Log on to the BEx Analyzer as REPORTING-##. Open queries from the *InfoAreas* tree. Notice the queries that appear. To see the owner of the query (*Created by*), choose *Properties On/Off*. Select a specific query to see the

Continued on next page

 © 2006 SAP AG. All rights reserved.

properties of the query. You should now have access to the queries that your BW365-## created. Other queries may be displayed. These are queries where the *Created by* field of the query is blank.

Task 3:

When a user goes into the BEx Analyzer, you want them to only execute workbooks, not queries. If a user selects *Open → Queries*, you do not want the *InfoAreas* button to appear. Use authorization object S_RS_FOLD to accomplish this task.

1. Change your role, **REPORTING_BASIC_##**, inserting the authorization object S_RS_FOLD.
2. Read the documentation on S_RS_FOLD. Then update the *Hide 'Folder' Pushbutton* field and select the value *X, True*. Generate the authorization and accept the default profile name.
3. Log on to the BEx Analyzerr as REPORTING-##. Select *Open → Query* from the BEx toolbar. The *InfoAreas* button should not appear.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Solution 4: Using S_RS_COMP1 and S_RS_FOLD

Task 1:

Create your own role, called **REPORTING_BASIC_##**, by copying the REPORTING_BASIC role. In the new role, update the authorization for object S_RS_COMP1 to only see queries where BW365-## is the query owner.

1. As user BW365-##, copy role REPORTING_BASIC to a new role called **REPORTING_BASIC_##**. When prompted, choose *Copy Selectively* and accept all default values.
   a) As user BW365-##, to enter role maintenance follow the path *Tools → Administration → user maintenance → Role Administration Roles (transaction PFCG)* .
   b) In the *Role* field, enter **`REPORTING_BASIC`** and choose *Copy role*.
   c) In the *to role* field, enter **`REPORTING_BASIC_##`** and choose *Copy Selectively*.
   d) When prompted to choose which objects to copy, accept the defaults and choose *Enter*.
   e) Remain on this screen for the next exercise.
2. For your new role, **REPORTING_BASIC_##**, change the authorization information. On the *Authorizations* tab, update authorization object S_RS_COMP1 by changing the *Owner* field value from * to **BW365-##**.
   a) On the *Role Maintenance* screen, enter **`REPORTING_BASIC_##`** in the *Role* field and choose *Change role* (pencil icon).
   b) Select the *Authorizations* tab and choose *Change Authorization Data* from the lower part of the screen.
   c) Expand the *Business Information Warehouse* object class.
   d) Expand the authorization object *Business Explorer - Components: Enhancements to the Owner* (Object S_RS_COMP1).
   e) Choose *Change*, next to the *Owner (Person Responsible)* (RSZOWNER) field. Replace the existing value for this field with your power user ID, **`BW365-##`**. Save your settings and return to the previous screen.

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

3. Generate the role. Accept the default profile name.
   a) Select *Authorizations → Generate*. When prompted, accept the default profile name by choosing **Enter**.
4. Remove the role REPORTING_BASIC from the user REPORTING-## and give REPORTING-## your new role, **REPORTING_BASIC_##**. Do this by maintaining the user master record directly. When finished, REPORTING-## should only contain one role: REPORTING_BASIC_##.
   a) As user BW365-##, to access user maintenance follow the path *SAP menu → Tools → Administration → User Maintenance → Users* .
   b) In the *User* field, enter your user, **`REPORTING-##`**, and choose *Change*.
   c) Choose the *Roles* tab.
   d) Delete the REPORTING_BASIC role by highlighting the role and choosing *Delete Row*.
   e) Enter the role **`REPORTING_BASIC_##`** as a new entry. Your user should now have only one role: REPORTING_BASIC_## . Save your settings.

Task 2:

Log on to the BEx Analyzer as REPORTING-## and note which queries the user can access.

1. Log on to the BEx Analyzer as REPORTING-##. Open queries from the *InfoAreas* tree. Notice the queries that appear. To see the owner of the query (*Created by*), choose *Properties On/Off*. Select a specific query to see the properties of the query. You should now have access to the queries that your BW365-## created. Other queries may be displayed. These are queries where the *Created by* field of the query is blank.
   a) Log on to the BEx Query Designer as REPORTING-##. If you are already logged in as REPORTING-##, close and logon again using *Start → Programs → Business Explorer→ Business Explorer→ Analyzer.*
   b) Select *Open → Query* from the BEx toolbar.
   c) Select *InfoAreas*.
   d) Open up the InfoAreas that appear to see the queries.
   e) Select a query and choose *Display Properties* to see the owner (Created by).

      Access Display Properties using the context menu, on the selected query.

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Task 3:

When a user goes into the BEx Analyzer, you want them to only execute workbooks, not queries. If a user selects *Open* → *Queries*, you do not want the *InfoAreas* button to appear. Use authorization object S_RS_FOLD to accomplish this task.

1. Change your role, **REPORTING_BASIC_##**, inserting the authorization object S_RS_FOLD.
   a) As user bw365-## access role maintenance using transaction PFCG.
   b) In the *Role* field, enter **`REPORTING_BASIC_##`** and choose *Change role*.
   c) Choose the *Authorizations* tab.
   d) Choose *Change Authorization Data* from the lower part of the screen.
   e) Choose *Edit* → *Insert Authorizations.* → *Manual Input*.
   f) Enter **`S_RS_FOLD`** in the *Authorization Object* field and choose *Enter*.
2. Read the documentation on S_RS_FOLD. Then update the *Hide 'Folder' Pushbutton* field and select the value *X, True*. Generate the authorization and accept the default profile name.
   a) Select *Change* next to the *Hide 'Folder' Pushbutton* field and select *X, True*. This will place an **X** in the field value.
   b) Select *Authorizations* → *Generate*. If prompted, accept the default profile name by choosing *Enter*.
3. Log on to the BEx Analyzerr as REPORTING-##. Select *Open* → *Query* from the BEx toolbar. The *InfoAreas* button should not appear.
   a) Log on to the BEx Analyzerr as REPORTING-##.
   b) Select *Open* → *Query* from the top menu. The *InfoAreas* button should not appear. Your Reporting-## user can only display queries and workbooks assigned a role.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Lesson Summary

You should now be able to:

- Explain the options available for securing data access for reporting users.
- List the steps required for InfoObject-level security.
- Define security by InfoArea, InfoCube, and InfoObject.
- Limit security by query owner.

Related Information

Once you have created your analysis authorizations, they must be transported from your development system to your production system, unless you create them in the production system directly. You can assign authorizations to transport requests in transaction RSECADMIN.

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: How to Use BI-Specific Authorization Values

Lesson Overview

This lesson will discuss authorization values that are specific to BI.

Lesson Objectives

After completing this lesson, you will be able to:

- List authorization values that are specific to BI
- Define security for aggregated values
- Explain how to use variables in regards to authorizations

Business Example

You have set up security for the division InfoObject.and related it to an InfoCube. Now all queries on InfoProviders containg division are checked for authorizations. Even if a query does not use the division InfoObject, there is still summarized division data in the results set. You must enable the user to retrieve summarized division data when reporting on other characteristic InfoObject levels.

Being able to retrieve summarized data is also useful in a situation where users are authorized to see detailed data for a particular characteristic value, such as their assigned sales organization, but are only authorized to see summarized data for all other sales organizations.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Using a Colon (:) as an Authorization Value

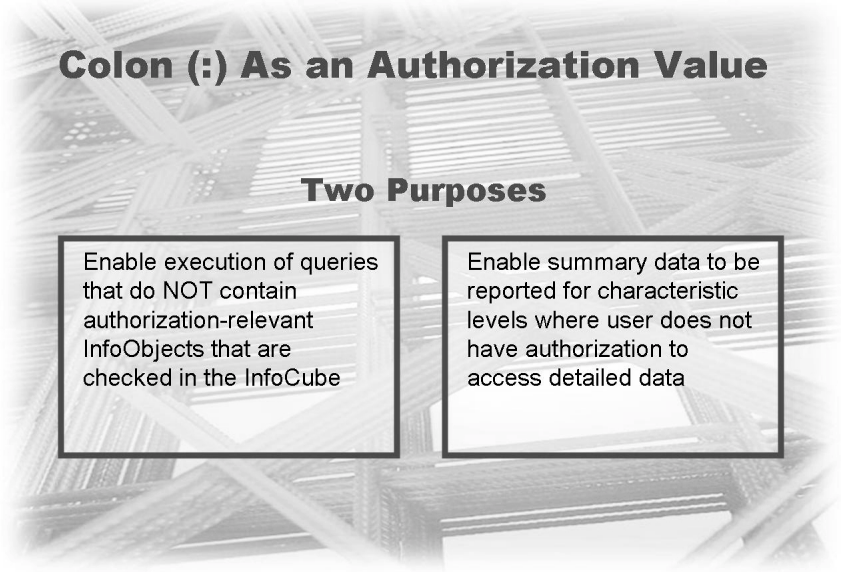


Figure 29: Two Purposes for Colon Authorization Value

If the InfoProvider has sensitive data, it could be that you do not want the user to see any summarized data. For example, let us assume you have an InfoProvider that has sensitive forecasting data. In this business scenario you have chosen to secure by InfoObjects (for example, Company Code). If you do not want a user with access to CompanyCode 1000 to see ANY data from other company codes, then you might not give this user the colon (:) value in the authorization. This would mean that ANY queries on your InfoProvider that do not use the CompanyCode InfoObject will fail for this user. That could be what you want, because in this example the ability to view any forecasting numbers for multiple company codes (even though the data is reported by country and cannot be viewed by company code), could compromise an aspect of your business.

Caution: Once an InfoObject is authorization relevant, ALL queries on all InfoProviders containing that InfoObject will be checked for authorization. Even if the InfoObject is not contained in such a query. Every query that does not use the secured InfoObject(s) will fail if the user does not have a ":" value or full authorization in their authorization.

Another purpose for the colon authorization value is highlighted in the following table. It is feasible that a sales manager is allowed to view the respective total sales figures for all sales organization, but is only authorized to break down their specific

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

sales organization (0001) according to the individual sales employees. In this case, the following authorizations, which are grouped together, would be created and assigned to the sales manager:

Sample Authorization Values

Authorization	Field	Value
Authorization 1	Sales organization Sales employee Key figure	* : **Sales figures**
Authorization 2	Sales organization Sales employee Key figure	**0001** * **Sales figures**

The user frequently uses these multidimensional authorities in companies that are regional as well as product-oriented (matrix organization). In this way, you could arrange for the person responsible for the combination of a certain division and a certain sales organization to have the exact authorization for the output of the relevant values, without necessarily also having access to the data for the whole division or the whole sales area.

Using a Pound Sign (#) as an Authorization Value

When data is loaded into SAP BW, some fields may be marked as “no value assigned” (posted with INITIAL). If you have secured an InfoObject that has data that is unassigned in the InfoCube, you may choose to give the user a pound sign (#) in order to avoid an authorization error at runtime.

The # character is interpreted as authorization for the display of the value *Not assigned* (posted with INITIAL).

Using Variables

There are two different ways variables are used for authorization processing. It is important to understand the differences.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Using Variables

Variable Type	Function	Special Authorization Value
Customer Exit	Dynamic granting of authorizations	**$<variable name>**
Authorization	Dynamic (automatic) filtering of queries	Not a matter of authorization values but used in query definition

Variables of type *Customer Exit* can be used with the special value **$** (as escape sequence) as prefix before the variable name. This enables dynamic granting of authorizations (authorized values are retrieved at runtime). This is a feature covered in detail when **maintenance of authorizations** is discussed.

Earlier we discussed that each InfoObject you are securing needs to be set up as a variable in the queries where the InfoObjects are used. This enables the query to receive a value, in our case a value for division.

Currently in our exercise scenario, every time you execute the query you must enter a division value. The variable that is used can be set up to read authorization data instead of prompting for values at query runtime. If the variable reads the authorization data, then a dialog box does not appear and the query results include all divisions for which the user is authorized. This type of variable is often called an **authorization variable**.

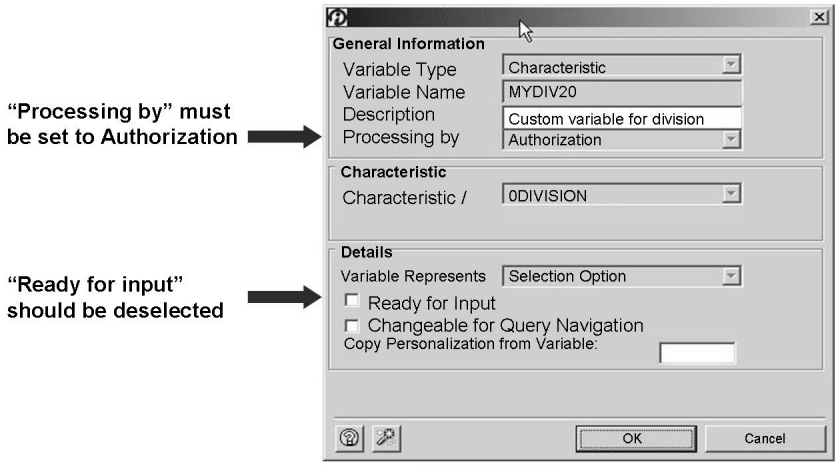


Figure 30: Division Variable of Type Authorization

© 2006 SAP AG. All rights reserved.

The variable needs to be set up to have the *Processing by* parameter set to **Authorization**. Additionally, the *Ready for Input* checkbox should NOT be selected if the query user should automatically receive data for all values for which they are authorized. If the *Input Ready* checkbox is selected, the user gets a dialog box for entering the desired characteristic values. With F4 help or the down arrow, however, only the values for which the user is authorized are called.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Exercise 5: Using BI-Specific Authorization Values

Exercise Objectives

After completing this exercise, you will be able to:

- Demonstrate how the colon (:) is used as an authorization value

Business Example

There are other queries for InfoCube **T_365SD##**. You need to ensure those queries can provide summary data for division.

Task 1:

Note: During the course of these exercises, if you cannot select the *InfoAreas* button in the BEx Analyzer, or you cannot see all the queries you expect, you may need to return to your role, **REPORTING_BASIC_##**, update the *owner field* on S_RS_COMP1 to an (*), and remove or inactivate object S_RS_FOLD.

As user Reporting-## execute your first query **Sales Report ##**. Do not enter a division when prompted!

Does the query execute successfully?

1. As user **REPORTING-##**, execute your first query (Sales Report GR##). What happens? Why?

Task 2:

As user BW365-##, change your analysis authorization, **ZDIV##**, by adding **:** as an additional value for the *BW365 Division* field. Then execute your first query again as user REPORTING-##.

1. In analysis authorization maintenance, update **ZDIV##**, by adding **":"** as an additional value for the *BW365 Division* field.
2. Execute your first query as user **REPORTING-##**. It should execute without any authorization errors.

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Task 3:

Create a query variable that automatically reads authorization data.

1. Log on to the BEx Analyzer as user BW365-##. Access your Sales Report GR## query, **T_365_GR##_Q1**, in change mode.
2. Add a new variable for InfoObject BW365 Division that is processed by authorizations. Use the following values in the Variable Wizard tool:

Field in the Wizard	Value to enter
Description	`GR## Division`
Technical Name	`GR##DIV`
Processing by	`Authorization`
Variable Represents	`Selection Option`
Variable is Ready for Input	`Deselected` (no check mark)

Task 4:

Update your query, **T_365_GR##_Q1**, to use your new authorization variable. Execute your query as user REPORTING-##.

1. Remove the current variable on the Division InfoObject.
2. Add the GR## Division variable you created to the Division InfoObject in the Filter area. Save and close the query when finished.
3. Log on to the BEx Analyzer as user REPORTING-## and execute your Sales Report query, *T_365_GR##_Q1*. You should no longer be prompted to enter the division. Drill down by division to ensure that only division 01 results are reported.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Solution 5: Using BI-Specific Authorization Values

Task 1:

Note: During the course of these exercises, if you cannot select the *InfoAreas* button in the BEx Analyzer, or you cannot see all the queries you expect, you may need to return to your role, **REPORTING_BASIC_##**, update the *owner field* on S_RS_COMP1 to an (*), and remove or inactivate object S_RS_FOLD.

As user Reporting-## execute your first query **Sales Report ##**. Do not enter a division when prompted!

Does the query execute successfully?

1. As user **REPORTING-##**, execute your first query (Sales Report GR##). What happens? Why?

   a) Log on to the BEx Query Designer as **REPORTING-##**

   b) Execute your first query, *Invoice Report GR##* . You can access the query by entering the name in the *Description / Technical Name* field and choosing *Enter*, or through the *InfoAreas* menu.

   c) The execution of the query will fail. Even though the *Division* field is not in the query, there is still data for all the divisions represented in the query results. The user currently only has access to division 01, so the user is not allowed to see summary data for all divisions.

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Task 2:

As user BW365-##, change your analysis authorization, **ZDIV##**, by adding **:** as an additional value for the *BW365 Division* field. Then execute your first query again as user REPORTING-##.

1. In analysis authorization maintenance, update **ZDIV##**, by adding **":"** as an additional value for the *BW365 Division* field.
   a) As user BW365-##, follow *Business Explorer → Manage Analysis Authorizations* to access analysis authorization maintenance.
   b) Select the *Authorizations* tab and choose *Maint.*.
   c) Enter your *Analysis Authorization* **ZDIV##.**
   d) Choose *Change* and press *YES* if prompted on the next screen.
   e) Highlight **T_DIV_365** add choose *Details*.
   f) Insert a row by pressing the + icon. Choose **I** in the Include/Exclude column. Choose **EQ** in the Operator Column. Enter a **:** in the technical characteristic column. Save. Go Back. Save. When prompted respond with YES.
2. Execute your first query as user **REPORTING-##**. It should execute without any authorization errors.
   a) Log on to the BEx Analyzer as REPORTING-##. If you are already logged on, close and reconnect as user REPORTING-##.
   b) Execute your query, **Invoice Report GR##**, found in the *History* listing. It should execute without any authorization errors now.

Task 3:

Create a query variable that automatically reads authorization data.

1. Log on to the BEx Analyzer as user BW365-##. Access your Sales Report GR## query, **T_365_GR##_Q1**, in change mode.
   a) Log on to the BEx Analyzer as user BW365-##, close and reconnect if necessary.
   b) Select *Open →Query* from the BEx toolbar.
   c) Turn on technical names by choosing *Technical Name On/Off*.
   d) Your query, **T_365_GR##_Q1**, should be in your *History* listing. Select the query and choose *Tools →Edit query* from the BEx Toolbar.

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

2. Add a new variable for InfoObject BW365 Division that is processed by authorizations. Use the following values in the Variable Wizard tool:

Field in the Wizard	Value to enter
Description	**`GR## Division`**
Technical Name	**`GR##DIV`**
Processing by	**`Authorization`**
Variable Represents	**`Selection Option`**
Variable is Ready for Input	**`Deselected`** (no check mark)

   a) On the left side of the *Query Designer* screen is a list of the InfoCube contents. Expand the tree structure by choosing *Sales area data → BW365 Division*.

   b) Expand BW365 Division. From the context menu for *Characteristic Value Variables* choose *New Variable*. A new panel will open on the right side of the Query Designer. Enter the above information into the corresponding fields. Take note that some of the required fields are on the *Details* tab of the variable and choose the *Save* icon at the top.

Task 4:

Update your query, **T_365_GR##_Q1**, to use your new authorization variable. Execute your query as user REPORTING-##.

1. Remove the current variable on the Division InfoObject.

   a) Select the *BW365 Division* variable under the Division InfoObject. Delete it by selecting *Remove* from the context menu.

2. Add the GR## Division variable you created to the Division InfoObject in the Filter area. Save and close the query when finished.

   a) Press Filter.

   b) From the context menu for Division, select *Restrict.*

   c) In the Show window, select *Variables*. Move your GR## Division variable from the left to the right by highlighting your variable and pressing the right arrow.

   Now Save!

Continued on next page

 © 2006 SAP AG. All rights reserved.

3. Log on to the BEx Analyzer as user REPORTING-## and execute your Sales Report query, *T_365_GR##_Q1*. You should no longer be prompted to enter the division. Drill down by division to ensure that only division 01 results are reported.

   a) Log on to the BEx Analyzer as REPORTING-##.

   b) Select *Query* → *Open* from the toolbar.

   c) Execute your query, **T_365_GR##_Q1**, found in the *History* listing. You should no longer be prompted to enter the division. In the query results, choose filter and drill down by division. Only division 01 results are reported.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- List authorization values that are specific to BI
- Define security for aggregated values
- Explain how to use variables in regards to authorizations

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Defining Security Using Hierarchies

Lesson Overview

This lesson will demonstrate how to set up security for hierarchies.

Lesson Objectives

After completing this lesson, you will be able to:

- Explain how hierarchies are used in BI.
- Explain why security is necessary for hierarchies.
- Demonstrate how to secure hierarchies.

Business Example

Your BI team will be using hierarchies for their data. You need to secure the data presented in queries by hierarchy node. Managers in the company are responsible for certain cost centers that have been assigned to particular business areas defined along country lines. Cost centers have been set up in BI within a country business area hierarchy. Sales managers in Great Britain should be able to see the portion of the cost center hierarchy for Great Britain, but they should not be able to see the portion of the hierarchy for Germany or any other country.

Hierarchies in BI

A hierarchy is a method of displaying characteristic values structured and grouped according to individual evaluation criteria. For example, you could easily envision cost centers grouped by country or region, or materials grouped by material type or material group. Hierarchies can be created in mySAP ERP and brought over to BI, or they can be created directly in BI. The following figure shows a hierarchy for cost centers by country and business area expanded to the cost center level.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Details of a Hierarchy

CO area 1000 Business Areas	0HIER_NODE
IDES BA Germany	0HIER_NODE
Business area 1000	0HIER_NODE
Motorcycle Sales	0COSTCENTER
Pump Sales	0COSTCENTER
Paints and Solvents Sales	0COSTCENTER
Light Bulb Sales	0COSTCENTER
Motorcycle Production	0COSTCENTER
Motorcycle Assembly	0COSTCENTER
High-Performance Pump P	0COSTCENTER
Pump Assembly	0COSTCENTER
Chemical Product Product	0COSTCENTER
Scrap Paints	0COSTCENTER
Bulb Production Line 1000	0COSTCENTER
Bulb Production Line 2000	0COSTCENTER
Business area 2000	0HIER_NODE
Elevator Sales	0COSTCENTER
Turbines	0COSTCENTER
Elevator Assembly	0COSTCENTER
Turbine Preassembly	0COSTCENTER

Figure 31: Cost Center Hierarchy Example

From a security perspective, we can assign authorizations to nodes in a hierarchy. In the figure, you can see nodes for country and business area. By assigning authorization at the node level, we could use the country node, or the country + business area node. For example, you can grant access to all the cost centers assigned to Germany, or only to business area 1000 in Germany.

Hierarchy security can be setup multiple ways. Examples include enabling the user to see the entire hierarchy, only the nodes, or the subtree below the nodes.

Hierarchies may be an integral part of your BI implementation. You will need to meet with the business team to determine if security is required for hierarchies and, if so, which hierarchies and which nodes. Creating and maintaining BI hierarchies is the responsibility of the BI developers. From a security perspective, we need to enable security on a hierarchy.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Steps to Implement Security on the Hierarchy Level

In order secure hierarchies, there are several steps:

1. Make the InfoObject on which the hierarchy is based authorization-relevant. For example, if the hierarchy is based on cost centers, then *0COSTCENTER* should be marked authorization-relevant.
2. Create an analysis authorization to protect the hierarchy using the InfoObject.

   Note: You don't have to create separate authorizations for hierarchical and non-hierarchical data. You could also enhance an existing (value) authorization with hierarchy authorizations.

3. Grant authorizations for hierarchy nodes to meet business needs to the users.

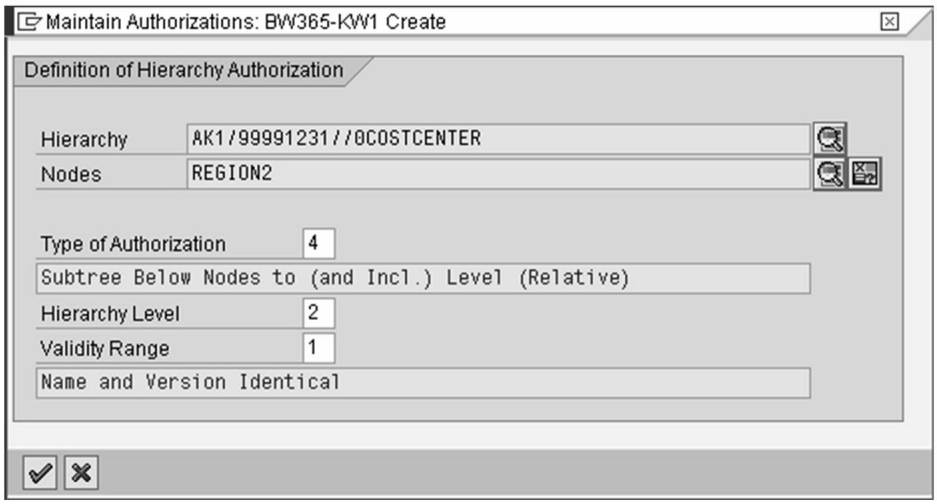


Figure 32: Hierarchy Authorization

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Maintaining Authorizations for Hierarchies

Note: Authorizations for hierarchies determine up to what level a user may drill down to in a hierarchy. This means that only data of the characteristic value sub-hierarchy is displayed when executing a query.

1. When creating an analysis authorization choose the InfoObject the hierarchy is based on as characteristic/dimension.
2. To create hierarchy node authorizations, in the detail maintenance choose the tab *Hierarchy Authorization*.
3. Create a hierarchy authorization and select the hierarchy and node.
4. Select the *Type of authorization*:

Type of authorization	
0	for the node
1	for a subtree below the node
2	for a subtree below the node up to and including levels for a subtree below the node.
3	for the entire hierarchy
4	for a subtree below the node up to and including levels (relative). (You have to specify a level that is defined relative to the node. It makes sense to specify a relative distance if an employee may only expand the hierarchy to a certain depth below his initial node, but this node is moved to another level when the hierarchy is restructured.)

5. Optionally you can use the following fields:

Continued on next page

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Field Name	How Used
Top of hierarchy	This option allows you to select the top of the hierarchy instead of a node in the hierarchy. If, for example, you want to authorize a user to work with a hierarchy from the top node, down to a particular level, you can of course authorize the user for the highest node in the hierarchy. If, on the other hand, the hierarchy is used in the query without a filter set for this node, the user is not able to execute the query. This is because the node that is displayed at the highest level in the hierarchy, is not actually the top of the hierarchy. For example, there is the 'All Other Leaves' node. This is an internal node, but a node in the hierarchy nevertheless, and it is this node that is at the top of the hierarchy, a level higher than the highest node that appears in the hierarchy display. If the hierarchy is used in the query, and the top-level node has not been specified explicitly, the system checks the authorization against the highest node in the hierarchy, meaning the internal node that is not displayed. This option, therefore, allows you to determine the top-level node of the hierarchy yourself, so that you can ensure that users are assigned the appropriate authorizations.
Hierarchy level	Within the framework of the authorization check, you can use this value to specify to which level the user can expand the hierarchy. Please note that this is an absolute value if the type of authorization is **2** and refers to the entire hierarchy. The highest node of a hierarchy stands at level 1. If you have entered the value 3 for the hierarchy level, for example, then the user can expand/see the hierarchy up to level 3. If you have chosen **4** as type of authorization the chosen node stands at level 1 and you can drill down to the number of levels specified here.
Area of Validity	0: Name, Version, and key Date identical 1: Name and version identical 2. Name identical 3: All hierarchies

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Exercise 6: Query Authorizations for Securing Hierarchies

Exercise Objectives

After completing this exercise, you will be able to:

- Assign to a user the correct authorizations for reporting using a hierarchy

Business Example

Whenever a user executes a query involving cost centers, the user should only have access to their assigned cost centers. Cost centers have been set up in a hierarchy. Each business area manager is only allowed to access the portion of the hierarchy that applies to their business area.

Task 1:

Ensure that the InfoObject T_CC_365 is marked as authorization-relevant.

1. In the InfoObject portion of the DataWarehousing Workbench, check if InfoObject T_CC_365 is marked as authorization-relevant.

Task 2:

Create an analysis authorization to protect the cost center hierarchy.

1. Start by creating an analysis authorization with the technical name **ZHIER##** and the description **Secure GR## CC Hier** . To do this, follow the path *SAP Menu → Business Explorer → Manage Analysis Authorizations*.
2. Maintain the authorization fields for the Analysis Authorization, **ZHIER##**. Include *T_CC_365* and the Special Characteristics (0TCAACTV, 0TCAINPROV, TCAVALID), in your authorization. Save your settings.

Task 3:

Define the authorization for the cost center hierarchy.

1. Make the necessary settings to link the **T_CA1000_BUSAREAS_GR##** hierarchy to the *T_CC_365* InfoObject. You want to limit access to the *Great Britain* node of the hierarchy with a *Type of authorization* value of *1*.

   From the *Definition for Hierarchies* screen, choose your CC Hierarchy, *T_CA1000_BUSAREA_GR##,*

Continued on next page

 © 2006 SAP AG. All rights reserved.

Task 4:

Test your new authorization for its access to the hierarchy.

1. Test your new Hierarchy Analysis Authorization by logging on as user REPORTING-##. Start the BEx Analyzer, find the query **CCA Hierarchy Report GR##** , and execute it.

   Only the Great Britain node of the hierarchy should appear in the results.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Solution 6: Query Authorizations for Securing Hierarchies

Task 1:

Ensure that the InfoObject T_CC_365 is marked as authorization-relevant.

1. In the InfoObject portion of the DataWarehousing Workbench, check if InfoObject T_CC_365 is marked as authorization-relevant.
   a) As user BW365-##, follow *SAP Menu → Modeling → Object Maintenance→InfoObject*.
   b) Enter **T_CC_365** in the InfoObject field and choose *Display.*
   c) Choose the *Business Explorer* tab. Notice that the *Authorization Relevant* checkbox is selected. If it is not selected, please inform your instructor.

Task 2:

Create an analysis authorization to protect the cost center hierarchy.

1. Start by creating an analysis authorization with the technical name **ZHIER##** and the description **Secure GR## CC Hier** . To do this, follow the path *SAP Menu → Business Explorer → Manage Analysis Authorizations*.
   a) As user BW365-##, follow the path *SAP menu → Business Explorer → Manage Analysis Authorizations* to access Analysis Authorization maintenance.
   b) From the Authorization tab, choose *Maint.*
   c) In the Authorization field enter **ZHIER##**.
   d) Choose *Create*.
   e) Enter a short, medium and long text of **`Secure GR## CC Hier.`**

Continued on next page

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

2. Maintain the authorization fields for the Analysis Authorization, **ZHIER##**. Include *T_CC_365* and the Special Characteristics (0TCAACTV, 0TCAINPROV, TCAVALID), in your authorization. Save your settings.

   a) On the *Maintain Authorization* screen, choose *Insert Row (*the + icon).

   b) Enter **T_CC_365**.

      Also, make sure you add the special characteristics using the appropriate icon.

   c) Highlight the T_CC_365 row and choose *Details*.

   d) Select the Hierarchy Authorization tab and then choose *Create.*

Task 3:

Define the authorization for the cost center hierarchy.

1. Make the necessary settings to link the **T_CA1000_BUSAREAS_GR##** hierarchy to the *T_CC_365* InfoObject. You want to limit access to the *Great Britain* node of the hierarchy with a *Type of authorization* value of *1*.

   From the *Definition for Hierarchies* screen, choose your CC Hierarchy, *T_CA1000_BUSAREA_GR##,*

   a) From the *Definition for Hierarchies* screen, choose your CC Hierarchy, *T_CA1000_BUSAREA_GR##,*

      When entering the values for the *Hierarchy* and *Nodes* fields, use F4 (drop down) to select the proper values from the list. Do not type the hierarchy and hierarchy node names directly into the fields.

   b) Next select the *CC Hierarchy node* for Great Britain by using F4 (drop down) and then dragging *IDES BA Great Britain* from the left to the right side of the screen.

   c) Press Continue.

   d) Select *1 subtree below nodes* from the dropdown menu for Type of Authorization.

   e) Press the green checkmark, Adopt Definition of Hierarchy Authorization.

   f) Save and return. (Green arrow, back)

   g) Assign your new analysis authorization to your REPORTING-## user.

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Task 4:

Test your new authorization for its access to the hierarchy.

1. Test your new Hierarchy Analysis Authorization by logging on as user REPORTING-##. Start the BEx Analyzer, find the query **CCA Hierarchy Report GR##** , and execute it.

   Only the Great Britain node of the hierarchy should appear in the results.

   a) Log on to the BEx Analyzer as **REPORTING-##**. If you are already logged on, disconnect and reconnect.

   b) From the BEx toolbar, select *Open → Queries*.

   c) Execute the query with the description **CCA Hierarchy Report GR##** and the technical name **T_365_GR##_Q2**. You can find and execute the query by entering the description or technical name in the *Description / Technical name* field and choosing *Enter*. Or, you can select *InfoAreas* to display the InfoArea tree structure and follow *BW Training → BW Customer Training → BW365 Authorization → Group ## → BW365 CCA Cube Group ## → CCA Hierarchy Report GR##.* Select the query and choose *OK* .

   d) Business area *Great Britain* should be the only hierarchy node that appears in the query result.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Explain how hierarchies are used in BI.
- Explain why security is necessary for hierarchies.
- Demonstrate how to secure hierarchies.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Monitoring Analysis Authorizations (Trace Functions)

Lesson Overview

This lesson will discuss how to trace your analysis authorizations.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the purpose of the analysis authorization trace
- Use the trace function
- Explain how to read the trace results

Business Example

You have set up security for the division InfoObject. A sales manager contacts you with a security error. You need to do a trace of what happened with the analysis authorizations. The problem is not with the delivered authorization objects, but with the analysis authorizations you created.

Using the Trace

There are two primary transaction codes that can be used to trace authorizations: ST01 and RSECADMIN.

Transaction code ST01 is a system trace that is used for SAP-provided objects. Transaction code RSECADMIN is specific to BI and only traces the custom reporting authorization objects you create to control access to InfoObject values. This trace can be very helpful when you need to debug an authorization error.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

The following are the procedure steps to trace custom reporting authorization objects using transaction code RSECADMIN.

1. Execute transaction code RSECADMIN.
2. Choose the tab*Analysis*.
3. There are two possibilities to trace:
   a) Choose the button *Error Logs*, add the user to the list and ask the user to run the query.
   b) Choose the button *Execution as ...*, type the user name, check *With Log* and execute the query yourself.
4. From this point on, the analysis authorization checks will be traced.
5. To look at the trace results, use the *Display* button in *Error Logs* after selecting the right log with the value help.

Hint: The first option (adding the user to the list of logged users) can be used permanently if legal auditing is required.

Protocol Overview

The protocol will be persisted on the database in an XML-based format and can be displayed in a readable form as HTML-Page. Consequently, it can be saved or printed like that. It is portable and can be viewed with any HTML-viewer.

1. The authorization checks are performed only for analysis authorizations.
2. All other authorization checks that are not administered in analysis authorization framework are checked for the executing (power) user with two exceptions: S_RS_COMP which is also checked for the restricted user and S_TCODE which is checked for the transaction that is called (e.g. RSRT).
3. The executing user needs corresponding permissions on the authorization object S_RSEC to execute the transaction as other user. If this authorization is missing the password of the restricted user is required to authenticate the execution.

The HTML page consists of several blocks that deal with a certain event during the authorization check which may be called in transactions amongst which are LISTCUBE, document maintenance as well as the standard case, the query execution for reporting or planning. To understand which kinds of authorization checks may occur, it makes sense to understand the query logics in terms of authorizations.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

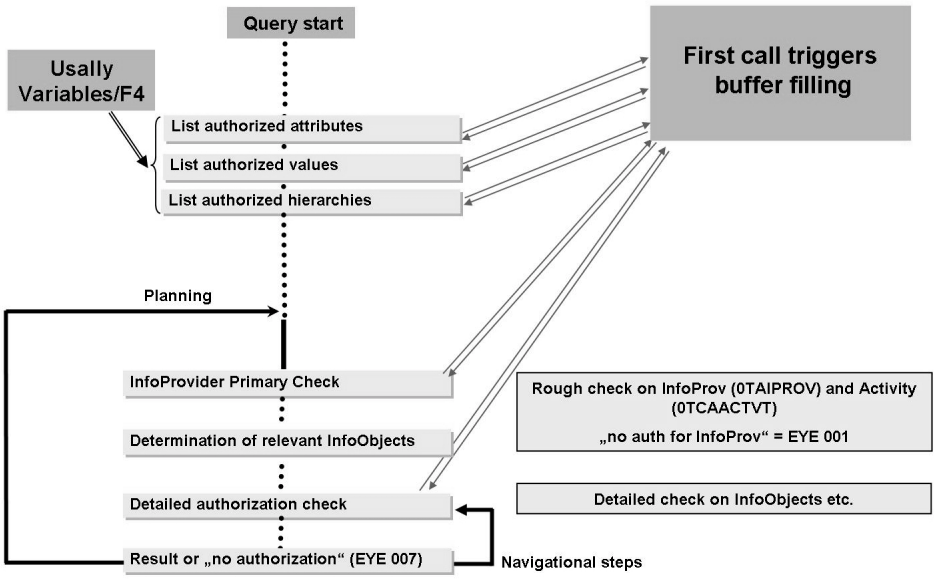


Figure 33: Query and Authorization Checks

- Query starts
- List of authorized attribute is requested
- Variable processing and Value Help (F4): Hierarchy authorizations and value authorizations are requested. Each request results in an individual block.
- Before checking for the details of the displayed data, the system checks for the authorization to the InfoProvider with a certain activity. If access is granted, the more detailed checks follow. Otherwise the query results in a message “No authorization to InfoProvider ...” (Message EYE001)
- Then the list of authorization relevant characteristics of the InfoProvider is determined
- As a last step the access to selected data in a certain naviagtional step is checked always if necessary. If this check fails, there are some combinations for selected data are not authorized. A message “No sufficient authorizations” (EYE 007)
- In planning the InfoProvider specific checks are repeated for different activities

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Details of the Protocol

To see which information can be extracted from the protocol, we will go more into detail of the protocol view which correspond to the steps described above.

- Protocol Header
- InfoProvider Check
- Attributes
- Value Authorizations
- Hierarchy (Node) Authorizations
- Relevant Characteristics
- Detailed Checks
- Buffer Filling, Pre-Optimizations

Protocol Header

At the beginning of each protocol there is a header that contains time and date of the executed authorization check, if available query name and InfoProvider name, the name of the user who has executed the query and possibly the name of the restricted user which may be different if the query was executed by a power user with analysis authorizations for another user. A time stamp (with the execution time on the local server and the time of the server of execution) and the calling transaction is listed. All the following blocks are separated by header lines with an underlying color.

InfoProvider Check

As a first check the system checks whether any of the authorization that is valid has the required combination of InfoProvider and Activity. This is nothing else than a check for a sufficient combination on the mandatory InfoObjects 0TCAIPROV (InfoProvider), 0TCAACTVT (Activity) and 0TCAVALID (Validity of the authorization). A frequent mistake is to forget the validity which effects in an invalid authorization that is not taken into account at all. The message in case of no authorization is “No authorization for InfoProvider with Activity...”

Hint: The message number and class is EYE 001 from which one can see that the problem is located in the combination of the three special mandatory characteristics 0TCAVALID, 0TCAIPROV, and 0TCAACTVT. As long as there is no access to the InfoProvider it does not make sense to spend time on the analysis of other details of the authorizations. At this point no (semantical) characteristic values or key figures have been checked, yet.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Attributes

During execution of a query there usually is always a check for the attributes which are authorized for an InfoObject. They are displayed in a table which also contains information on the attributes, whether it is just a display attribute (DIS) or a navigational attribute (NAV).

Hint: For display attributes that are authorization relevant, the full authorization is required (*). Otherwise the attribute will be hidden from the system (query design and execution).

Value Authorizations

The next block(s) cover(s) the value authorizations. Here the list for authorized values on a characteristic is presented. It is possible to check whether this the expected result. In some cases the authorized values are displayed as integer numbers, so-called surrogate Ids or in short SIDs. This may be the case in some cases where also leaves of hierarchy nodes are required.

Caution: Value authorizations are always combined from all valid authorizations for the current InfoProvider (if you are in an InfoProvider-context, which for a query is always the case). This means that all values from all authorizations for this InfoProvider are put together into the list of authorized values.

Hierarchy (Node) Authorizations

Here the list of authorized nodes is given together with some more technical information on the authorizations such as Authorization Type, Level, Validity Scope, together with information on the selected hierarchy itself.

Relevant Characteristics

This section is quite basic and helpful for analysis of authorization issues. In this section the list of characteristics that are actually relevant for the authorization checks is determined. It is the list of all characteristics that are marked as authorization relevant in the InfoObject maintenance, including Navigational Attributes reduced by those ones for which the user has full authorizations (*). Full authorization means in all combinations (=authorizations), not only in some. The user then has always full access to the transactional data which is related to the characteristic. This list is an optimization in order to avoid processing of characteristics for which the user has full access.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Detailed Checks

This section is the most detailed one. It contains information on the detailed combinatorical checks of selections against the authorizations.

Caution: Always bear in mind that the selected set of data must be a subset of the authorized data. Authorizations do not automatically work as query filters.

This section starts with some preparations as a consistency check of nodes and intervals. The selection is separated into various sub-selections, which carry a number (SUBNR). This structure will reflect in several sub-sections of checks which may fail individually. After the preprocessing section, the main checks will repeatedly start again for each SUBNR structure.

Aggregation Check and Aggregation Authorization

As a first step, in for every sub-selection it is checked whether a check for aggregation authorization is necessary which depends on the navigational state. Since at this point, the aggregation check is not yet part of the selection, it must be added here. All characteristics that are authorization relevant but not in drill down or even not in the query (but in the InfoProvider) must be authorized with aggregation authorization (:). this aggregation authorization is missing here.

Caution: If aggregation checks are performed you need to have aggregation or full authorization for the characteristic. This is a frequent causeof authorization failure.

Set Comparison

Next step is the comparison of all sub-selections (SUBNR) with all authorizations that are assigned and valid today and valid for the InfoProvider (if relevant as in query context). The algorithm for a single SUBNR is as follows:

1. Compare selection set with all authorizations and find out, whether the selected set is a subset of (or equal to) the authorization set.

   Yes: Selection is authorized

   No: calculate the authorized part (intersection of selection with authorization) and the non-authorized rest set. Put the rest set to the list of selection parts that still must be checked. (it might be that the rest set is authorized by another authorization)
2. If any selection or rest set is left, go to step 1 again.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Buffer Filling, Pre-Optimizations

All information on authorizations are usually required several times, for example during navigational steps or even for several value helps on authorization relevant InfoObjects. Since the preparing steps that must or may be done before actual authorization processing take a certain amount of time, all necessary information is buffered at the first call. The most important steps of this buffering are extension and merging of authorizations which means summarizing authorization that can enhance each other. Extension adds authorizations for characteristics that are not included in an authorization from other authorizations. Merging summarizes authorizations that differ in one dimension (one characteristics).

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Exercise 7: Tracing BI Authorizations

Exercise Objectives

After completing this exercise, you will be able to:

- Trace the authorizations.

Business Example

You are authorizing access by the BW365 division InfoObject. You have set up security, but the users are getting errors even though everything seems to be correct in the setup. You want to trace the object at runtime to help you fix the errors.

Task:

As user BW365-##, turn on the trace for user REPORTING-##.

1. In RSECADMIN add user REPORTING-## to the users being logged.
2. As user REPORTING-##, execute your query, *T_365_GR##_Q1*.
3. As BW365-##, return to the *Error Logs* in RSECADMIN. Select the log for your user from the value help.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Solution 7: Tracing BI Authorizations

Task:

As user BW365-##, turn on the trace for user REPORTING-##.

1. In RSECADMIN add user REPORTING-## to the users being logged.
   a) As BW365-##, choose tab *Analysis* and button *Error Logs*.
   b) Select the button *configure log recording*.

      Choose *Add User*.
   c) Enter REPORTING-## and save.
2. As user REPORTING-##, execute your query, *T_365_GR##_Q1*.
   a) Log on to the BEx Analyzer as REPORTING-##.
   b) From your *History* listing, execute the query *T_365_GR##_Q1*.
3. As BW365-##, return to the *Error Logs* in RSECADMIN. Select the log for your user from the value help.
   a) As BW365-## in transaction RSECADMIN choose *Analysis* and *Error Logs*.
   b) Press the *delete selections* button, then enter **`Reporting-##`** in the *Restricted user* field, press *Enter* and then press the *display* icon. Select the appropriate log by double clicking it.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Describe the purpose of the analysis authorization trace
- Use the trace function
- Explain how to read the trace results

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Important Aspects of BI Authorizations

Lesson Overview

This lesson introduces general aspects of authorizations in the BI area. It gives a high-level overview of BI specific considerations that are important when it comes to designing or implementing BI authorizations.

Lesson Objectives

After completing this lesson, you will be able to:

- Understand the most important aspects of BI authorizations on an overview level.
- Avoid common misunderstandings with BI authorizations.

Business Example

You would like to get a general idea of how to map your business requirements in regards to authorizations to the BI capabilities.

Overview about Aspects

[Enter a title and the conceptual information about this lesson in this section. You can also include additional sections, graphics, demonstrations, procedures, and/or simulations.

Differentiate Standard and Analysis Authorization

	Standard Authorizations	Analysis Authorizations
Allow access to	Meta data Objects (InfoProvider = *0SD_C01*)	Semantical data slices (company code = *1200*)
Typical use	Object Maintenance, data access on a coarse level	Granular access to data slices / subsets of data
Structure designed by	SAP	Customer

Standard Authorizations are the ones based on structures delivered by SAP. They allow users to perform administration tasks or to create, change or delete meta data objects like InfoObjects or InfoCubes. SAP pre-configures the structure of the authorizations and implements the authorization check. This is done by means of authorization objects in the object class Business Information Warehouse.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Granting the authorization to the users is the customer's only responsibility. Standard authorizations in other basis authorization object classes also cover authorizations for e.g. calling a transaction or user management like in all NetWeaver systems.

Analysis Authorizations define semantic data slices a user is allowed to see in reporting, like all data belonging to company code *1200*. The structure and values are not pre-configured by SAP but completely customer-defined. It is the customer's responsibility to define the components (InfoObjects) that are relevant for the authorization checks. In previous releases the authorizations were based on customer-defined authorization objects. In NetWeaver 2004s, authorizations are defined directly with completely flexible structure. This type of authorization is BI-specific.

While there are clearly defined differences between the two types of authorizations they enhance each other. They can also partially replace each other. Example: You can create a query *Travel costs* containing a fixed filter on company code *1200*. Using standard authorizations you can give a user access to that query (as meta data object). This query can display data for company code *1200* only, even without restricting analysis authorizations for company code. In simple scenarios this kind of securing data can be sufficient, however, in most scenarios maintenance effort would be too high and security requirements could not be met.

Differentiated Design Time / Maintenance and Runtime

Defining the right authorization approach is a matter of minimizing the impact on development and maintenance without compromising security requirements. How authorizations are grouped in roles or profiles or direct assignment, whether they are generated or maintained manually is a very important topic when it comes to cost of maintenance. However, the query runtime environment is separated from authorization maintenance. The authorization check at query runtime needs the set (union) of all authorizations that are assigned to a user, independent of how they have been assigned.

Variables, initially designed to filter queries dynamically (at query runtime) can also be used for flexible authorization maintenance. Differentiate between these two functions of the variables.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Differentiate Runtime and Design / Maintenance

	Query Runtime	Maintenance
Authorizations	The union of all authorizations is checked independent of grouping or assignment method	Grouping of authorizations (e.g. in roles), assignment method chosen are important for ease of maintenance
Variables	Query is filtered dynamically with variables of any type (e.g. type authorization)	*$<variable name>* logic can be used for flexible authorization granting but does not automatically filter a query Available for customer-exit variables

Differentiate Query Selections and Analysis Authorizations

A selection in a query contains a set of filters on characteristics. Users or administrators often expect query selections to automatically match the user's authorizations, i.e. the users should see exactly all the data they are authorized for. While this can typically be achieved, it is not automatically done. There is no direct link between a query and analysis authorizations. You have to enable the queries to be filtered in a way so they can match the authorizations and don't fail the authorization check. This is achieved by means of fixed filters or variables (dynamic filters).

A selection cuts a rectangular subset out of all possible combinations of characteristic value. Even more precisely, a query selection accesses the Cartesian product of the filters on the individual characteristics. The same is true for one authorization.

 © 2006 SAP AG. All rights reserved.

However, if a user has two or more authorizations, the union of these authorizations cannot always be combined into one (because the union is not necessarily rectangular), see graphical example.

- Query Selections
  - Belong to query
  - Are defined by fixed and dynamic filters
  - Are checked at runtime for matching analysis authorizations
  - Is a rectangular subset of the multi-dimensional space
- Analysis Authorizations
  - Are defined independent of queries
  - Union of authorizations may be a complex structure (not rectangular)

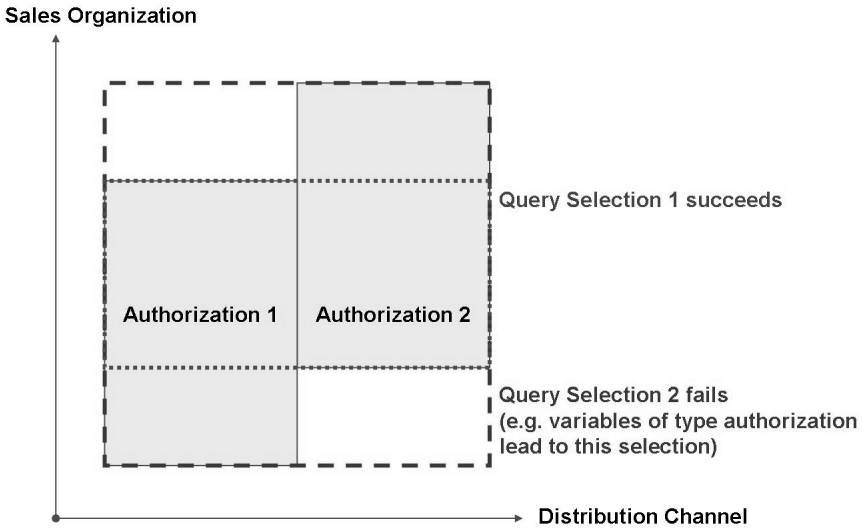


Figure 34: Example: Multi-Dimensional Query Selections and Analysis Authorizations

In the graphic the union of the two authorizations cannot be fully covered in one query selection. If a user had these authorizations assigned, the rectangular superset of the authorizations in a query selection would result in an authorization check failure. The subset selection would not fail the authorization check but it fails to display all authorized values. This is an example where the expectation to display all authorized values cannot be met, at least not with one selection.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

If you use variables of type authorization (filled automatically with authorized values) for both characteristics in the example, the query filters the query according to the union of all values, thus authorization check fails. You can find more information and another example in other lessons of this course.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Understand the most important aspects of BI authorizations on an overview level.
- Avoid common misunderstandings with BI authorizations.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Tracing Authorizations

Lesson Overview

In this lesson, we will learn how to use transaction code ST01 to trace standard authorizations. How to trace analysis authorizations will be discussed later.

Lesson Objectives

After completing this lesson, you will be able to:

- Explain the purpose of the ST01 trace in regards to authorizations
- List the differences between ST01 and the trace for analysis authorizations

Business Example

You either need to find out what authorizations are required to perform a certain activity on the system or you would like to find out why a user has insufficient authorizations for an activity he/she is entitled to perform.

Purpose of SAP Trace Tools

SAP provides two primary trace tools for debugging security problems. Transaction code ST01 executes a trace tool that exists on all ABAP based systems. Among other purposes, this tool serves as trace for all SAP-provided authorizations objects. You simply turn on the trace (for a specific user), and when the trace is completed you can see which authorization objects were checked and the results of the check.

In transaction RSECADMIN →*Analysis* you can execute a trace that is specific to BI analysis authorizations. Analysis authorizations will not appear in the ST01 trace.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

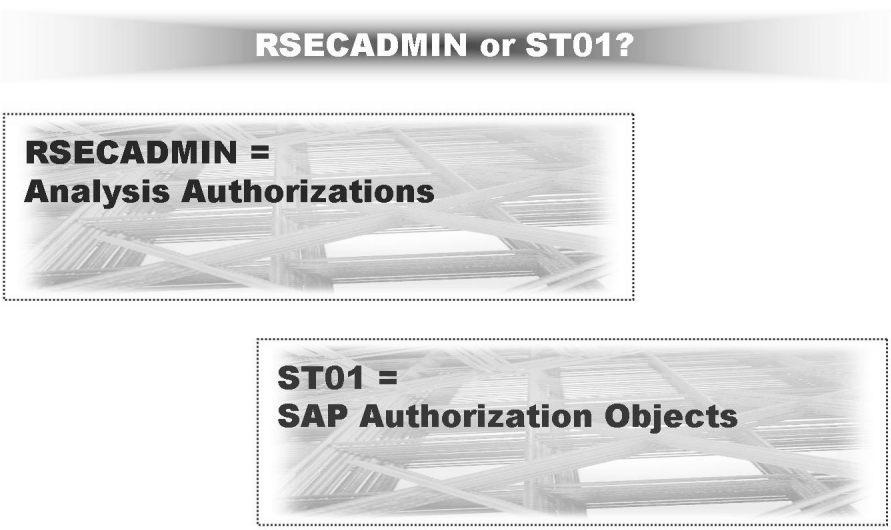


Figure 35: Using Trace Tools

Using the ST01 Trace Tool

If you want to use the ST01 trace tool, you only have to activate the trace and filter for a specific user. To do this use, *Edit → Filter → General* in transaction code ST01.

When you do the analysis on the trace, you will see a darker shade highlighting security checks that were successful, and a lighter shade highlighting security checks that failed. To get more information on a specific line in the trace log, simply double-click on the line.

Do not be surprised to see many entries for authorization objects S_RS_COMP and S_RS_COMP1. Since those objects are checked when building the list of queries displayed in the BEx Analyzer tool, all InfoAreas and InfoCubes you do not have access to will appear in the lighter shade.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

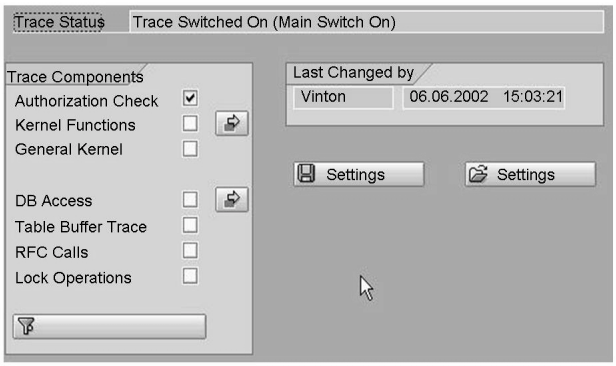


Figure 36: ST01 Trace Tool

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Exercise 8: ST01 Trace

Exercise Objectives

After completing this exercise, you will be able to:

- Demonstrate using ST01 trace for an administrative user

Business Example

You have a user who needs the ability to create InfoCubes. You want to know exactly what authorization objects are checked when creating an InfoCube.

Task 1:

Make sure the trace has been turned on for your class.

1. As user BW365-##, follow *SAP Menu → Tools → Administration → Monitor → Traces → System Trace* or use transaction code ST01. Make sure the trace is active for authorization checking. After the trace, deactivated it again.

Task 2:

Create an InfoCube while the trace is turned on. Then analyze the trace file.

1. In the *InfoProvider* portion of the DataWarehousing Workbench, create an InfoCube with a technical name **MYCUBE##** and a description of **GR## My Cube** in your own InfoArea, **T_BW365_GR##**. Copy your existing InfoCube, **T_365SD##**. Activate the new InfoCube.
2. Follow *SAP Menu → Tools → Administration → Monitor → Traces → SAP System Trace* or use transaction code ST01 to return to the system trace. Display the analysis from the trace file and filter the results for your own user ID. The trace file should contain entries for the authorization object S_RS_ICUBE.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Solution 8: ST01 Trace

Task 1:

Make sure the trace has been turned on for your class.

1. As user BW365-##, follow *SAP Menu → Tools → Administration → Monitor → Traces → System Trace* or use transaction code ST01. Make sure the trace is active for authorization checking. After the trace, deactivated it again.

   a) As user BW365-##, follow *SAP Menu → Tools → Administration → Monitor → Traces → System Trace* or use transaction code ST01.

   b) Ensure the trace component *Authorization check* is selected.

   c) Choose *Edit → Filter → Shared* to ensure that no filter is set.

   d) Select the *change trace* button to activate the trace.

Task 2:

Create an InfoCube while the trace is turned on. Then analyze the trace file.

1. In the *InfoProvider* portion of the DataWarehousing Workbench, create an InfoCube with a technical name **MYCUBE##** and a description of **GR## My Cube** in your own InfoArea, **T_BW365_GR##**. Copy your existing InfoCube, **T_365SD##**. Activate the new InfoCube.

   a) As user BW365-##, follow *SAP Menu → Modeling → DataWarehousing Workbench: Modeling*.

   b) Choose *Modeling → InfoProvider* on the left side of the screen if it is not already displayed by default.

   c) Under the *InfoProviders* window, follow *BW Training → BW Customer Training → BW365 Authorization → Group ##*. Select your InfoArea, **Group ##**. Then right-click and select *Create InfoCube*.

   d) For the *InfoCube* name, enter **`MYCUBE##`**.

   e) For the description, enter **`GR## My Cube`**.

   f) In the *Copy from* field, enter **`T_365SD##`**.

   g) Choose *Create*.

   h) Choose *InfoCube → Activate* to activate your new InfoCube.

Continued on next page

 © 2006 SAP AG. All rights reserved.

2. Follow *SAP Menu → Tools → Administration → Monitor → Traces → SAP System Trace* or use transaction code ST01 to return to the system trace. Display the analysis from the trace file and filter the results for your own user ID. The trace file should contain entries for the authorization object S_RS_ICUBE.

   a) Follow *SAP Menu → Tools → Administration → Monitor → Traces → System Trace* or use transaction code ST01.

   b) Choose *Analysis*.

   c) Enter your user ID, BW365-##, in the *User name* field.

   d) In the *Trace Records* section, limit the records to only those for *Authorization check*.

   e) Select *Start reporting* to view the trace file. Look for authorization object S_RS_ICUBE.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Explain the purpose of the ST01 trace in regards to authorizations
- List the differences between ST01 and the trace for analysis authorizations

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Unit Summary

You should now be able to:

- Define the purpose of Analysis Authorizations.
- Describe how to create an Analysis Authorization.
- Describe how to incorporate an Analysis Authorization into a role./
- Explain the options available for securing data access for reporting users.
- List the steps required for InfoObject-level security.
- Define security by InfoArea, InfoCube, and InfoObject.
- Limit security by query owner.
- List authorization values that are specific to BI
- Define security for aggregated values
- Explain how to use variables in regards to authorizations
- Explain how hierarchies are used in BI.
- Explain why security is necessary for hierarchies.
- Demonstrate how to secure hierarchies.
- Describe the purpose of the analysis authorization trace
- Use the trace function
- Explain how to read the trace results
- Understand the most important aspects of BI authorizations on an overview level.
- Avoid common misunderstandings with BI authorizations.
- Explain the purpose of the ST01 trace in regards to authorizations
- List the differences between ST01 and the trace for analysis authorizations

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Test Your Knowledge

1. Which of the following is not an option for securing reporting users?

   Choose the correct answer(s).

   - □ A Secure by InfoArea
   - □ B Secure by InfoCube
   - □ C Secure by InfoObjects
   - □ D Combination of A, B, and C
   - □ E Secure by query name
   - □ F Secure by source system

2. Which of the following are steps to securing reporting users by InfoObjects?

   Choose the correct answer(s).

   - □ A Create analysis authorizations with the InfoObjects you wish to secure.
   - □ B Create variables for queries that use the secured InfoObjects.
   - □ C Mark the InfoObject authorization-relevant.
   - □ D Link your analysis authorization to an InfoProvider.

3. RSSM is the transaction code used to create security for InfoObjects used in queries.

   Determine whether this statement is true or false.

   - □ True
   - □ False

4. S_RS_COMP1 enables you to limit access to queries by query owner.

   Determine whether this statement is true or false.

   - □ True
   - □ False

5. Creating variables for queries that use the secured InfoObject is a requirement for efficient implementation of InfoObject-level security.

   Determine whether this statement is true or false.

   - □ True
   - □ False

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

6. The colon (:) value should be used in your authorizations for custom objects if aggregated values for an authorization relevant characteristics are displayed in a query.

   Determine whether this statement is true or false.

   □ True

   □ False

7. If you do not want someone to drill down on an authorization relevant characteristic, then use the (:) value only.

   Determine whether this statement is true or false.

   □ True

   □ False

8. When would you use the $ in an authorization value?

   Choose the correct answer(s).

   □ A If you are using a customer-exit variable to fill the authorization values at runtime

   □ B If you have cost centers that start with $

   □ C Anytime you want to grant all values; $ is like * in standard authorizations

   □ D If you want to filter the queries with authorized values

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

9. Which best describes how to set up security for hierarchies?

   Choose the correct answer(s).

   - □ A Create an analysis authorization that includes the InfoObject for the hierarchy (example: 0COSTCENTER). Create a variable for the queries that provides which node values the user will be able to access. Insert your authorization into a role and assign it to the users.
   - □ B Create an authorization object that includes the InfoObject for the hierarchy (example: 0COSTCENTER). Link this object to an InfoProvider. Insert your authorization into a role and specify the node the user will access.
   - □ C Create an analysis authorization that includes the InfoObject for the hierarchy (example: 0COSTCENTER). Create the hierarchy authorization within the analysis authorization that provides which node values the user will be able to access. Assign your authorization to the users.
   - □ D Create an analysis authorization that includes the InfoObject for the hierarchy (example: 0COSTCENTER). Mark the hierarchy as authorization relevant. Assign the authorized nodes to the users.

10. Hierarchies are used in BI to rank employees.

    Determine whether this statement is true or false.

    - □ True
    - □ False

11. Securing a hierarchy enables you to secure a node and everything below the node.

    Determine whether this statement is true or false.

    - □ True
    - □ False

12. The trace in transaction code RSECADMIN traces activities with S_RS_COMP.

    Determine whether this statement is true or false.

    - □ True
    - □ False

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

13. To use the trace in transaction RSECADMIN, you need to enter the object you want to trace.

    Determine whether this statement is true or false.

    □ True

    □ False

14. When looking at the trace results, you will see your relevant analysis authorizations and check marks for successful authorization checks.

    Determine whether this statement is true or false.

    □ True

    □ False

15. The ST01 trace is used to trace analysis authorization objects created in transaction code RSECADMIN.

    Determine whether this statement is true or false.

    □ True

    □ False

16. The ST01 trace can be used in both a BI and a mySAP ERP system.

    Determine whether this statement is true or false.

    □ True

    □ False

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Answers

1. Which of the following is not an option for securing reporting users?

   Answer: F

   Reporting users can be secured by combinations of InfoArea, InfoCube, query name, and InfoObject, but not by source system. Source systems are secured in the administration area of SAP BW.

2. Which of the following are steps to securing reporting users by InfoObjects?

   Answer: A, B, C

   Analysis authorizations are not linked to an InfoProvider, the InfoProvider is specified in the analysis authorization itself.

3. RSSM is the transaction code used to create security for InfoObjects used in queries.

   Answer: False

   RSSM is the transaction used for the old authorization concept in SAP BW 3.5 and below. The main transaction for analysis authorizations is RSECADMIN.

4. S_RS_COMP1 enables you to limit access to queries by query owner.

   Answer: True

   S_RS_COMP1 includes a field that limits access by query owner.

5. Creating variables for queries that use the secured InfoObject is a requirement for efficient implementation of InfoObject-level security.

   Answer: True

   Inserting variables in queries makes the query much more flexible. You do not have to create multiple versions of the same query to handle different selection criteria. Since the variable can access the authorized values for a user, it is a very efficient way to implement InfoObject-level security.

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

6. The colon (:) value should be used in your authorizations for custom objects if aggregated values for an authorization relevant characteristics are displayed in a query.

   Answer: True

   You need the colon for each authorization relevant characteristic you display aggregated values for. This enables queries to execute that do not explicitly use the characteristics. Full authorizations (*) include the colon authorization. You don't have to specify the colon in addition to full authorizations.

7. If you do not want someone to drill down on an authorization relevant characteristic, then use the (:) value only.

   Answer: True

   The colon implies summary values only.

8. When would you use the $ in an authorization value?

   Answer: A

   The $ implies that the customer-exit variable fills the authorizations dynamically.

9. Which best describes how to set up security for hierarchies?

   Answer: C

   Hierarchy authorizations are defined directly within the analysis authorization. Analysis authorization can be assigned either directly to the users or in a role.

10. Hierarchies are used in BI to rank employees.

    Answer: False

    Hierarchies are used to order data in a hierarchical fashion.

11. Securing a hierarchy enables you to secure a node and everything below the node.

    Answer: True

    If you are using hierarchies, then security by the hierarchy is an efficient way to implement security. By granting access to the hierarchy node, the user will get all data below the specified node.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

12. The trace in transaction code RSECADMIN traces activities with S_RS_COMP.

    Answer: False

    The trace in RSECADMIN only records analysis authorizations.

13. To use the trace in transaction RSECADMIN, you need to enter the object you want to trace.

    Answer: False

    You need to enter the user ID you want to trace in transaction RSECADMIN.

14. When looking at the trace results, you will see your relevant analysis authorizations and check marks for successful authorization checks.

    Answer: True

    When you look at the trace results, you will see green check marks for successful checks.

15. The ST01 trace is used to trace analysis authorization objects created in transaction code RSECADMIN.

    Answer: False

    Transaction code ST01 only traces SAP-provided authorization objects.

16. The ST01 trace can be used in both a BI and a mySAP ERP system.

    Answer: True

    The ST01 trace is available in all ABAP based systems.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Unit 4

Saving BEx Objects to BI Roles

Unit Overview

This unit discusses the security requirements when saving BEx objects to a role.

Unit Objectives

After completing this unit, you will be able to:

- Describe the difference between workbooks and queries.
- Explain security that surrounds workbooks.
- Add workbooks to roles.

Unit Contents

Lesson: Securing Workbooks 132
Exercise 9: Securing Access to Workbooks 139

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Securing Workbooks

Lesson Overview

This lesson will explain how to secure Workbooks. End users may save query results to workbooks, which are linked to query definitions. In this lesson, we will describe the difference between workbooks and queries and explain how to secure workbooks.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the difference between workbooks and queries.
- Explain security that surrounds workbooks.
- Add workbooks to roles.

Business Example

Once a user navigates and formats the query results to suit their needs, they may want to save the results in a workbook. The user can save the workbook in a *Role* folder so that it is easy to call it up again later on. Saving a workbook to a Role also means that other users, who have the same role, can execute the workbook. For example, if the sales manager for the northern regions wants to make a workbook accessible to a sales manager from the southern region, the workbook can be accessible by both managers if it is saved in a role that is common to both managers.

You must set up security to control who can save workbooks, where they can be saved, and which workbooks appear in the BEx Analyzer for a specific user.

Comparison of Workbooks and Queries

Our focus in this class has been to launch the BEx Analyzer, select a query, and execute that query. The query then provides a result. A drilldown or formatting or results did not occur, instead we discussed the security involved with allowing a user to execute a query and display results.

An SAP BI user spends more time on the results. They perform activities such as drilling down to various levels in the data, rearranging the results to highlight certain relationships in the data, and optionally saving the results to a workbook. Now that the user has spent that time to format the results in a meaningful way, they would like the results to be in the same format each time they retrieve the results. To accomplish this, the user does not execute a query, but instead executes a workbook. The workbook

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

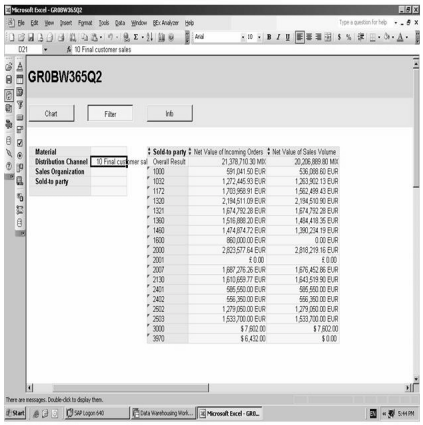
contains the results of the query in the formatted look and feel that the user requires. Data in a workbook can either be static, refreshed manually, or refreshed automatically when the workbook is retrieved.

Queries are actually inserted into workbooks so you can display them. A workbook could contain several queries that are related in nature.

Thus, a query is more the technical definition of what the results should look like. Workbooks are actual results that have been formatted and can be refreshed each time the workbook is executed.

The query is a definition of what data the query should fetch and how the data should be initially displayed. A query definition includes rows, columns, filters, and free characteristics.

Sales filtered by Division 10.



Sales filtered by Sales Organization 1000

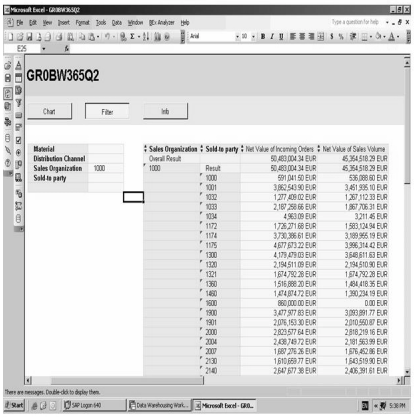


Figure 37: Query Results Can be Saved to Workbooks

The workbook is a result set of the query. In this workbook, the data is displayed by sales organization. Every time the user executes the workbook, the data will be refreshed, but the format can remain the same, depending on the settings for the query in the workbook.

The workbook above is from the same query definition, but here the results are displayed differently. The results are displayed by division.

Multiple query results saved in workbooks from the same query definition enable users to customize how they want to review the results and analyze the data.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Saving Workbooks to Roles

If a user wants to save a workbook to a location where it can be easily accessed by others, they need to save to a *Role*. Saving to a *Role* means saving to a security role.

You may want to set up roles specifically for saving workbooks. You can then assign the role to all parties who need to share workbooks. For example, if a sales manager in the northern region and a sales manager in the southern region need to execute the same workbooks, they will both have the role you created to hold those sales workbooks. When the manager for the southern region creates a new workbook, the manager will save it to the role for sales workbooks. This enables the manager in the northern region to execute the new workbook.

Another option is only allowing power users to save workbooks to maintain the roles and ensure that the workbooks remain manageable. This also prevents users from changing workbooks saved by other users. In the example above, if sales managers from all regions can save workbooks, then a sales manager for the southern region could change a workbook created by the sales manager in the northern region.

In order to save workbooks to roles, a user needs:

- **S_USER_AGR**: Authorizations: Role check
- **S_USER_TCD**: Transactions in roles

The authorization object S_USER_AGR has two fields: *Activity* and *Role Name*. For the *Activity* field, the user must have at least values **01**, **02** and **22**. If the user can delete workbooks, they will also need value **06**. For the *Role Name*, you should enter the specific roles you have created for saving workbooks.

It might seem surprising to see activities 01 (Add or Create) and 02 (Change) for the object S_USR_AGR. Object S_USER_AGR is required so the user can save the workbook to the *Menu* area of the role. When granting access to S_USER_AGR, you need to grant create and change authorizations for a specific role name. The role name is the name of a role that will be used to hold workbooks. When a workbook is saved in a role, the area *Menu* for a role is changed. Thus the object S_USER_AGR is a required object.

Authorization object S_USER_TCD has one field, *Transaction Code*. The user needs value **RRMX** in this field.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Authorization objects:

S_USER_AGR

S_USER_TCD

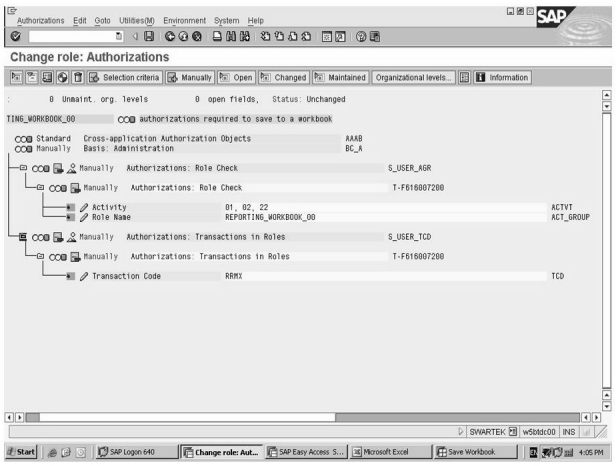


Figure 38: Authorizations to Save Workbooks to a Role

As a part of the security implementation plan, determine who can save workbooks to roles and how the roles for workbooks should be organized. The workbook security strategy should include who will need to save workbooks, what roles will they use, and how the roles will be shared.

Caution: For security reasons, it is recommended that workbooks be refreshed when opened to ensure that data from the last execution is not displayed. To refresh workbooks when opening select from the BEx Analyzer Menu: *Workbook Settings→ General → Refresh Workbook on Open*.

From the BEx toolbar choose:

Save Workbook as.

Choose *Role.*

Choose the folder.

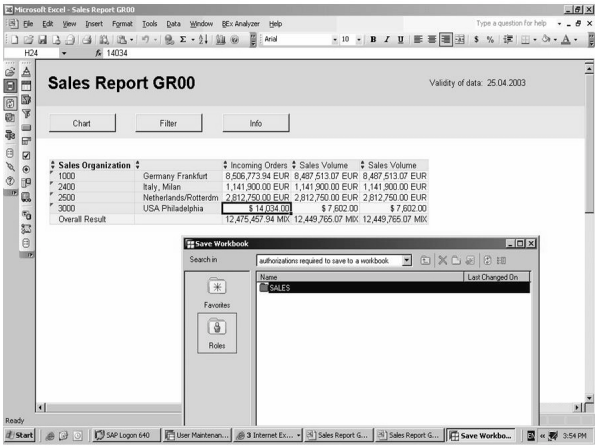


Figure 39: Save a Workbook to a Role from the BEx Analyzer

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

With the proper authorization, users can save workbooks to a role from the BEx Analyzer.

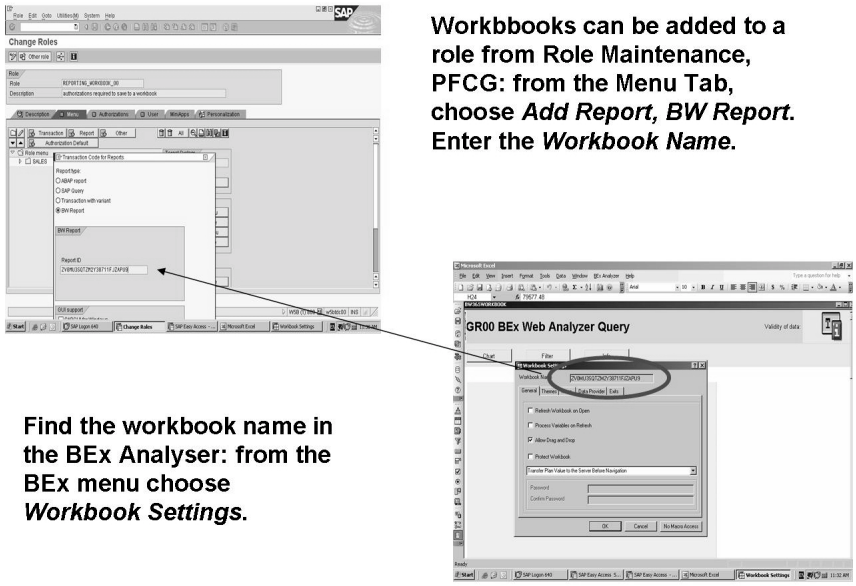


Figure 40: Save Workbooks to a Role Menu from Role Maintenance

Security Administrators, with access to PFCG, can save workbooks to a role menu. After creating a folder, insert a workbook by choosing *Add Report.* Enter the technical name of the report. Find the technical name of the workbook in the BEx Analyzer. From the BEx menu choose *Workbook Settings.*

Note: The BI Workbook directory tables are RSRWBINDEX and RSRWBINDEXT.

TRANSPORTING ROLES WITH WORKBOOKS

For a role to be used, it must be saved to a role. When the role is assigned to a user, the user has access to the workbook. Many business content roles have attached workbooks. For example, the Business Content role, SAP_BW_TCONT has the BI Statistics workbook attached to it.

Normally roles are created in development and moved to production. However, in a BI production environment some users can create a workbooks and save workbooks to a role. If that role originally came from DEV, and you make changes to the role in DEV and transport it again, that will remove the attachments for all the workbooks

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

that were saved to the role in production. The workbooks will still exist in production, but they will no longer be attached to the role, and the user will not be able to see the workbooks.

For the roles with workbooks, it probably will be best for the security administrator to create specific roles for workbooks that only contain workbooks with NO authorizations. Any changes made to the role will be from workbooks being created and saved to this role in a production environment. This role should be created in DEV and transported to PRD, but it should be empty and no other subsequent transports should occur for this role.

Note: Use report RSWB_REORG_ROLES to identify what workbooks are not attached to a role. Also, you can use this report to delete unused workbooks.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Exercise 9: Securing Access to Workbooks

Exercise Objectives

After completing this exercise, you will be able to:

- Demonstrate how reporting users execute workbooks using the BEx Browser
- Describe how workbooks appear in the BEx Browser
- Explain what security is required for saving workbooks

Business Example

The sales manager of the northern region executes a query and then refines the query results to meet a specific business need. The manager then wants to save the results so that when the query executes again, the results will appear in the same format. To accomplish this, the sales manager needs to save the results as a workbook. Additionally, the sales vice president wants to save a workbook so that the sales managers of the southern and western regions can execute the same workbook.

You need to secure who can create workbooks, and manage which users can execute specific workbooks.

Task 1:

As the user REPORTING-##, execute your query, *T_365_GR##_Q1*, and save the query as a workbook in your *Favorites* folder. Then try to save the query to your *Roles* folder.

1. Log on to the BEx Analyzer as REPORTING-##.
2. Execute your query, *T_365_GR##_Q1*. Do a drilldown by distribution channel.
3. Save the query as a workbook. Add the workbook into your *Favorites* folder. Name the workbook **GR## Distribution Channel Analysis**. Try to add the query to your *Role* folder.

Continued on next page

 © 2006 SAP AG. All rights reserved.

4. Why were you not able to save your workbook to your role? Is this a security problem?

_____
_____
_____
_____

Task 2:

As user BW365-##, verify that the role **REPORTING_WORKBOOK** has sufficient authorization to save query results as a workbook. Then, copy the role **REPORTING_WORKBOOK** to your own role, **REPORTING_WORKBOOK_##**. Add additional authorizations to be able to save your workbooks to a role. Add a folder, SALES, to your role menu. Assign your REPORTING-## user to your new role, REPORTING_WORKBOOK_##.

1. Display the role **REPORTING_WORKBOOK**. Verify that this role provides the basic access needed to save workbooks to your *ROLES* folder.
2. Copy **REPORTING_WORKBOOK** to your own role, **REPORTING_WORKBOOK_##**.
3. In the **REPORTING_WORKBOOK_##** role, go to the *Authorizations* tab and manually insert the objects S_USER_AGR and S_USER_TCD. Provide the following field values:

Authorization Object	**Field**	**Value**
S_USER_AGR	*Activity*	`01, 02, 22`
S_USER_AGR	*Role Name*	`Reporting_WORKBOOK_##`
S_USER_TCD	*Transaction Code*	`RRMX`

4. In your role definition, access the *Menu* tab and create a folder, **SALES**.
5. Via role maintenance, assign user REPORTING-## to your new role, **REPORTING_WORKBOOK_##**. Then display the user master record for REPORTING-##, verifying that you understand the function of each role assigned.

Continued on next page

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Task 3:

As the user REPORTING-##, execute your query, *T_365_GR##_Q1*, drilling down on *Distribution channel*. Try to save the query to a workbook named **GR## Distribution Channel Analysis** in your *Roles* folder.

1. Log on to the BEx Analyzer as REPORTING-##. If you are already logged on, disconnect and reconnect to the BI server.
2. Execute your query, *T_365_GR##_Q1*. Do a drilldown by distribution channel.
3. Save the query to a workbook named **GR## Distribution Channel Analysis**. Try to put the workbook into your *Roles* folder.

Task 4:

Optional: As user BW365-##, look at role **REPORTING_WORKBOOK_##** to see how it has changed since the workbook was saved. Assign a workbook manually to the role.

1. Bring up your **REPORTING_WORKBOOK_##** role in change mode and select the *Menu* tab.
2. Expand the *Sales* folder. You will see your workbook assigned there.
3. To insert a workbook manually, choose *Add Report* and *BW Report*.
4. Notice the *Report ID* field. Enter the workbook ID (not the query name) found in the settings of the workbook, in this field. Rename the default workbook as **GR## Sales Manager Workbook**. Return to the *SAP Easy Access* menu for BI when finished.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Solution 9: Securing Access to Workbooks

Task 1:

As the user REPORTING-##, execute your query, *T_365_GR##_Q1*, and save the query as a workbook in your *Favorites* folder. Then try to save the query to your *Roles* folder.

1. Log on to the BEx Analyzer as REPORTING-##.
   a) From your workstation, choose *Start* → *Programs* → *Business Explorer* → *Analyzer*.
   b) If prompted enable macros.
   c) From the BEx toolbar, select *Open* → *Queries*.
   d) Log on as REPORTING-##.
2. Execute your query, *T_365_GR##_Q1*. Do a drilldown by distribution channel.
   a) Your query, named *Sales Report GR##* with technical name *T_365_GR##_Q1*, should be in your *History* listing. If not, enter the query name in the *Description/Technical Name* field. Double click on the query name to execute it.
   b) If you get a dialog box for the Division variable, enter **`01`**.
   c) In the top part of the query results, choose *Filter*. Double click on *Distribution Channel* to do a drilldown.
3. Save the query as a workbook. Add the workbook into your *Favorites* folder. Name the workbook **GR## Distribution Channel Analysis**. Try to add the query to your *Role* folder.
   a) From the BEx toolbar, select *Save* → *Save As Workbook*.
   b) Select the *Favorites* folder, enter **`GR## Distribution Channel Analysis`** in the *Description* field, and select *Save*. . In our example, this means that the sales manager for the northern region can now save workbooks to a *Favorites* folder, but cannot save a workbook to a location that can be easily accessed by the sales manager for the southern region.
   c) Now try to save the query to your *Role* folder

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

4. Why were you not able to save your workbook to your role? Is this a security problem?

   Answer: Saving the workbook to your *Role* folder should not work successfully. You may have received an error. When you click on that message, you may get another message that says, "Workbook was not saved." Your message may be different, but the result is that no workbook was saved.

   Your user must have authorization to save workbooks to the database. Additional authorization is required to be able to save workbooks to a role.

   .Verify that the Workbook was **not** saved by choosing *Open → Workbooks* from the BEx menu and selecting the *Role* folder.

   It is not apparent that this is a security problem, but it is. Your user currently has access to S_RS_COMP and S_RS_COMP1 but is not authorized to save workbooks to Roles.

   To save workbooks to Roles, a user must have access to authorization objects S_USER_AGR and S_USER_TCD. These authorizations protect roles.

Task 2:

As user BW365-##, verify that the role **REPORTING_WORKBOOK** has sufficient authorization to save query results as a workbook. Then, copy the role **REPORTING_WORKBOOK** to your own role, **REPORTING_WORKBOOK_##**. Add additional authorizations to be able to save your workbooks to a role. Add a folder, SALES, to your role menu. Assign your REPORTING-## user to your new role, REPORTING_WORKBOOK_##.

1. Display the role **REPORTING_WORKBOOK**. Verify that this role provides the basic access needed to save workbooks to your *ROLES* folder.

   a) As user BW365-##, choose *SAP menu → Tools → Administration → User Maintenance → Role Administration→Roles*.

   b) Enter **`REPORTING_WORKBOOK`** in the *Role* field and choose *Display*.

   c) Select the *Authorizations* tab and display the authorization data.

Continued on next page

 © 2006 SAP AG. All rights reserved.

2. Copy **REPORTING_WORKBOOK** to your own role, **REPORTING_WORKBOOK_##**.
   a) Choose *Back* to return to the *Role maintenance* screen.
   b) Enter **`REPORTING_WORKBOOK`** in the *Role* field and choose *Copy role* to copy the role.
   c) In the *to role* field, enter **`REPORTING_WORKBOOK_##`**. Choose *Copy All* and choose *Enter*.
   d) Change the description of your new role to **`GR## REPORTING WORKBOOK .`**
3. In the **REPORTING_WORKBOOK_##** role, go to the *Authorizations* tab and manually insert the objects S_USER_AGR and S_USER_TCD. Provide the following field values:

Continued on next page

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Authorization Object	Field	Value
S_USER_AGR	*Activity*	`01, 02, 22`
S_USER_AGR	*Role Name*	`Reporting_WORKBOOK_##`
S_USER_TCD	*Transaction Code*	`RRMX`

a) Select the *Authorizations* tab and choose *Change Authorization Data* from the lower part of the screen. Save the role if prompted by the system.

b) Choose *Edit* → *Insert Authorizations.* → *Manual Input*.

c) In the *Authorization object* field, add objects **`S_USER_AGR`** and **`S_USER_TCD`**. Choose *Enter*.

d) Expand the object class *Basis: Administration*.

e) Expand authorization objects *S_USER_AGR* and *S_USER_TCD*.

f) Choose *Change* next to each field and enter the authorization values listed below.

Authorization Object	Field	Value
S_USER_AGR	*Activity*	`01, 02, 22`
S_USER_AGR	*Role Name*	`Reporting_WORK-BOOK_##`
S_USER_TCD	*Transaction Code*	`RRMX`

g) Generate the profile by choosing *Authorizations* →*Generate.*

h) Change the name of the profile to **`SALESWB##`** and choose enter.

4. In your role definition, access the *Menu* tab and create a folder, **SALES**.

a) Select the *Menu* tab.

b) Select the entry named *Role menu* and choose *Create Folder*.

c) In the *Folder name* field, enter **`Sales`** and choose *Enter*.

Continued on next page

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

5. Via role maintenance, assign user REPORTING-## to your new role, **REPORTING_WORKBOOK_##**. Then display the user master record for REPORTING-##, verifying that you understand the function of each role assigned.

   a) In role **REPORTING_WORKBOOK_##**, select the *User* tab.

   b) In the *User ID* field, enter **`REPORTING-##`**.

   c) Select *User comparison*, choosing *Complete comparison* when prompted.

   d) Go to user maintenance: *SAP menu → Tools → Administration → User Maintenance → Users*.

   e) Verify that REPORTING-## has two roles: REPORTING_BASIC_## and REPORTING_WORKBOOK_##.

      Before continuing, review the roles by double-clicking on each one. Make sure you understand the function of each role.

Task 3:

As the user REPORTING-##, execute your query, *T_365_GR##_Q1*, drilling down on *Distribution channel*. Try to save the query to a workbook named **GR## Distribution Channel Analysis** in your *Roles* folder.

1. Log on to the BEx Analyzer as REPORTING-##. If you are already logged on, disconnect and reconnect to the BI server.

   a) From your workstation, choose *Start → Programs → Business Explorer → Analyzer*.

   b) If prompted enable macros.

   c) From the BEx toolbar, select *Open → Queries*.

   d) Log on as REPORTING-##.

2. Execute your query, *T_365_GR##_Q1*. Do a drilldown by distribution channel.

   a) Your query, named **Sales Report GR##** with technical name *T_365_GR##_Q1,*, should be in your *History* listing. If not, enter the query name in the *Description/Technical Name* field. Double click on the query name to execute it.

   b) If you get a dialog box for the Division variable, enter **`01`**.

   c) In the top part of the query results, choose *Filter.* Double click on *Distribution Channel* to do a drilldown.

Continued on next page

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

3. Save the query to a workbook named **GR## Distribution Channel Analysis**. Try to put the workbook into your *Roles* folder.
   a) From the BEx toolbar, select *Save* → *Save As Workbook*.
   b) Select the roles folder and expand it until you can choose the folder *SALES*. Enter **`GR## Distribution Channel Analysis`** in the *Description* field. Choose *Save*. The request should now be successful.
   c) Verify that the workbook was saved by choosing *Open* → *Workbooks* from the BEx menu. Choose *Roles*→ *Sales* , and open your new workbook, **GR## Distribution Channel Analysis.**

Task 4:

Optional: As user BW365-##, look at role **REPORTING_WORKBOOK_##** to see how it has changed since the workbook was saved. Assign a workbook manually to the role.

1. Bring up your **REPORTING_WORKBOOK_##** role in change mode and select the *Menu* tab.
   a) As user BW365-##, choose *SAP menu* → *Business Explorer* → *Authorizations* → *Maintain Roles*.
   b) Enter **`REPORTING_WORKBOOK_##`** in the *Role* field and choose *Change role*.
   c) Select the *Menu* tab.
2. Expand the *Sales* folder. You will see your workbook assigned there.
   a) Expand the *Sales* folder.
   b) You will see your workbooks. .
   c) If you turn on technical names by selecting *Turn on technical names*, you will see transaction code RRMX listed with the workbook. Additionally you can right-click on the workbook and select *Display details* to get more information.
3. To insert a workbook manually, choose *Add Report* and *BW Report*.
   a) To insert a workbook manually, choose *Add Report* and select the *BW Report* radio button.

Continued on next page

 © 2006 SAP AG. All rights reserved.

4. Notice the *Report ID* field. Enter the workbook ID (not the query name) found in the settings of the workbook, in this field. Rename the default workbook as **GR## Sales Manager Workbook**. Return to the *SAP Easy Access* menu for BI when finished.

   a) In order to insert a workbook ID, you must find the technical name assigned to the workbook. From the bottom portion of the BEx Analyzer, choose *Workbook Settings*.

   b) The Workbook name is on the top of the next screen.

   c) Highlight the workbook name and select **Ctrl + C** on the keyboard. Paste the workbook ID into the *Report ID* field in the role using **Ctrl + V** on the keyboard.

   d) Choose *Enter*.

   e) The workbook name in the role defaults to *Business Warehouse Report*. Choose *Change node text* and rename the workbook as **`GR## Sales Manager Workbook`**.

   f) Choose *Enter*.

   g) Save. Return to the SAP menu.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Describe the difference between workbooks and queries.
- Explain security that surrounds workbooks.
- Add workbooks to roles.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Unit Summary

You should now be able to:

- Describe the difference between workbooks and queries.
- Explain security that surrounds workbooks.
- Add workbooks to roles.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Test Your Knowledge

1. What is the difference between a workbook and a query?

_____

_____

_____

_____

2. Reporting users normally have queries assigned to their roles.

   Determine whether this statement is true or false.

   □ True

   □ False

3. Which of the authorization objects is **NOT** required to save your query results to a Role folder?

   Choose the correct answer(s).

   □ A S_RS_ADMWB

   □ B S_USER_AGR

   □ C S_USER_TCD

   □ D S_RFC

4. When saving a workbook in the BEx Analyzer, you can save to any role you choose.

   Determine whether this statement is true or false.

   □ True

   □ False

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

5. Which of the following best describes the steps to save a workbook to a role using role maintenance?

   Choose the correct answer(s).

   - □ A In Role Maintenance on the Menu tab, select “Insert Report”, “SAP BW report”, and enter the query descriptive name.
   - □ B From the BEx Analyzer menu, choose *Workbook Settings* and highlight the workbook technical ID. Then switch to role maintenance (PFCG) and in the “Menu” tab, choose “Insert Report”, “SAP-BW Report” and insert the technical ID of the workbook.
   - □ C Enter the transaction code in the “Menu” tab in role maintenance. Then enter the query name in the “Authorizations” tab.
   - □ D In Role Maintenance on the “Menu” tab, select “Insert Report”, “ABAP Report”, and enter the query name.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

Answers

1. What is the difference between a workbook and a query?

   Answer: A query is a definition of what rows and columns a query should return. A workbook holds the query results and includes formatting rules. With a workbook, you can execute one or more embedded queries and get the results in the format that you desire.

2. Reporting users normally have queries assigned to their roles.

   Answer: False

   Reporting users normally have workbooks assigned to their roles.

3. Which of the authorization objects is **NOT** required to save your query results to a Role folder?

   Answer: A

   Authorization object S_RS_ADMWB is not required to save a workbook to a role.

4. When saving a workbook in the BEx Analyzer, you can save to any role you choose.

   Answer: False

   When saving a workbook in the BEx Analyzer, you can only save to the roles you have access to with the authorization object S_USER_AGR.

5. Which of the following best describes the steps to save a workbook to a role using role maintenance?

   Answer: B

   From the BEx Analyzer menu, choose *Workbook Settings* and highlight the workbook technical ID. Then switch to role maintenance (PFCG) and in the “Menu” tab, choose “Insert Report”, “SAP-BW Report” and insert the technical ID of the workbook

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Unit 5

Securing Data Access for Administration Users

Unit Overview

In this unit we will focus on the SAP BI administrator. We will discuss who SAP BI administrators are, what they do, and options for securing administrators. This unit also discussed the system security requirements for BI.

Unit Objectives

After completing this unit, you will be able to:

- Explain how to secure Data Warehousing Workbench objects such as InfoProviders, Data Transfer Processes, DataSources, Open Hub Destinations and Process Chains.
- Describe how to secure remote activation of Business Content DataSources.
- Explain how to protect maintenance of Master Data and Documents.
- Briefly describe how to secure Information Broadcasting distribution and Data Mining Objects.
- List the two logon methods for BI and Enterprise Portals.
- Explain the required security set up for communication between BI and other systems.
- Explain the RFC destinations required.
- List the profiles used for system communication.

Unit Contents

Lesson: Securing Data Access for Administrators 156
Lesson: System Communication Security 173
Exercise 10: Inspect System Communication Setup 179

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson: Securing Data Access for Administrators

Lesson Overview

This lesson will describe how to secure data access for BI Administrators.

Lesson Objectives

After completing this lesson, you will be able to:

- Explain how to secure Data Warehousing Workbench objects such as InfoProviders, Data Transfer Processes, DataSources, Open Hub Destinations and Process Chains.
- Describe how to secure remote activation of Business Content DataSources.
- Explain how to protect maintenance of Master Data and Documents.
- Briefly describe how to secure Information Broadcasting distribution and Data Mining Objects.
- List the two logon methods for BI and Enterprise Portals.

Business Example

To ensure that the Data Warehousing solution represents the structure of your company and fulfills its requirements, you have to define an effective overall security strategy. This includes proper security to protect Data Warehousing Workbench objects. You need to build authorizations to protect these objects and assign these authorizations to the proper BI Administrators.

Securing Data Warehousing Workbench Objects

Administrators must have access to Data Warehousing Workbench objects, such as InfoProviders, Data Transfer processes, Process Chains, Reporting Agent objects, Open Hub destinations, and DataSources.

Administrators must also create and maintain many other DataWarehouing objects. Authorization object S_RS_ADMWB protects these objects. There are only 2 fields attached to this authorization object: Data Warehousing object, and activity. However, this authorization object secures many different Data Warehousing objects.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

S_RS_ADMWB	Authorizations for working with individual objects of the Data Warehousing Workbench.

There are only 2 fields in this Authorization Object:

- **DataWarehousing Object**
- **Activity**

However, there are many values available for the DataWarehousing Object.

Figure 41: Securing Data Warehousing Workbench Objects

Data Warehousing objects secured with S_RS_ADMWB:

- *SourceSys* (Source system)
- *InfoObject* (InfoObject)
- *Monitor* (Monitor)
- *ApplComp (*Application components)
- InfoArea (InfoArea)
- *Workbench* (Data Warehousing Workbench)
- *Settings* (Settings)
- *MetaData (*Metadata)
- *InfoPackag* (InfoPackage and InfoPackage Group)
- *RA_Setting* (Reporting Agent setting)
- *RA_Package* (Reporting Agent package)
- *DOC_META* (Documents for metadata)
- *DOC_MAST* (Documents for master data)

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

- *DOC_HIER* (Documents for hierarchies)
- *DOC_TRAN (*Documents for transaction data)
- *DOC_ADMIN* (Administration of document store)
- *CONT_ADMIN* (Administration of Content systems)
- *CONT_ACT* (Installation of Business Content)
- *BR_SETTING* (Broadcast settings other than your own settings, which have one of the following distribution types: Send e-mail, send to the portal, send to the printer.)
- *USE_DND* (Drag and Drop to InfoAreas and application components)
- *CNG_RUN* (Attribute change run)
- *REMOD_RULE* (Modeling Rule "Modeling Rule" for the remodeling tool)
- *IMG_BI (*BI-relevant activities in IMG)
- *OLAP_CACHE* (OLAP cache objects)
- *HPA_ZA* (BIA Monitor checks and activities)

S_RS_MPRO	Authorizations for working with MultiProviders and their subobjects
S_RS_ODSO	Authorizations for working with DataStore objects and their subobjects.
S_RS_ISET	Authorizations for working with InfoSets
S_RS_HIER	Authorizations for working with hierarchies
S_RS_IOMAD	Authorizations for processing master data in the Data Warehousing Workbench

Figure 42: Securing InfoProviders

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

The authorization object S_RS_ICUBE protects InfoCubes and the InfoCube sub-objects:

- Definition - Definition
- UpdateRule - Update rules
- Data -Data
- Aggregate - Aggregate
- ExportISrc - Export DataSource
- Chavlrel - Characteristic relations (planning relevant)
- Dataslice - Data slices (planning relevant)

Securing InfoCubes

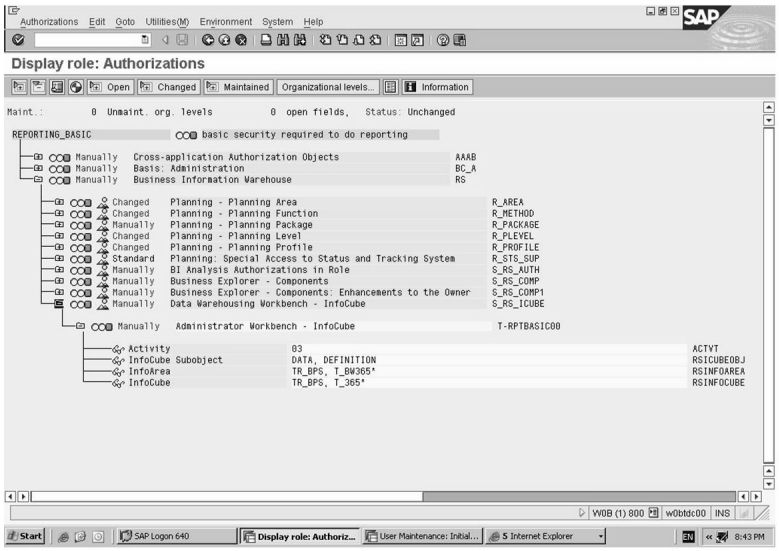


Figure 43: Securing InfoCubes

The authorization to secure datasources is S_RS_DS. This authorization object contains three fields:

- DataSource: the name of the DataSource that a user is allowed to edit.
- Source System: the source system for which a user is allowed to edit.
- SubObject for DataSource: Definition, Data, InfoPack.

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

S_RS_DS	Authorizations for working with the DataSource (Release > BW 3.x) or its subobjects.
S_RS_DTP	Authorizations for working with the data transfer process and its subobjects
S_RS_ISNEW	Authorizations for working with InfoSources (Release > BW 3.x)
S_RS_ISOUR	Authorizations for working with InfoSources with flexible updating and their subobjects
S_RS_ISRCM	Authorizations for working with InfoSources with direct updating and their subobjects
S_RS_TR	Authorizations for working with transformation rules and their subobjects

Figure 44: Securing Data Transfer Processes, InfoSources and DataSources

The authorizations assigned for the Data Transfer Process (DTP) object, S_RS_DTP, have a higher priority than the authorizations for the underlying objects. Users that have a DTP authorization for a source/target combination do not need read authorization for the source object or write authorization for the target object to execute the DTP.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Securing InfoSources and DataSources

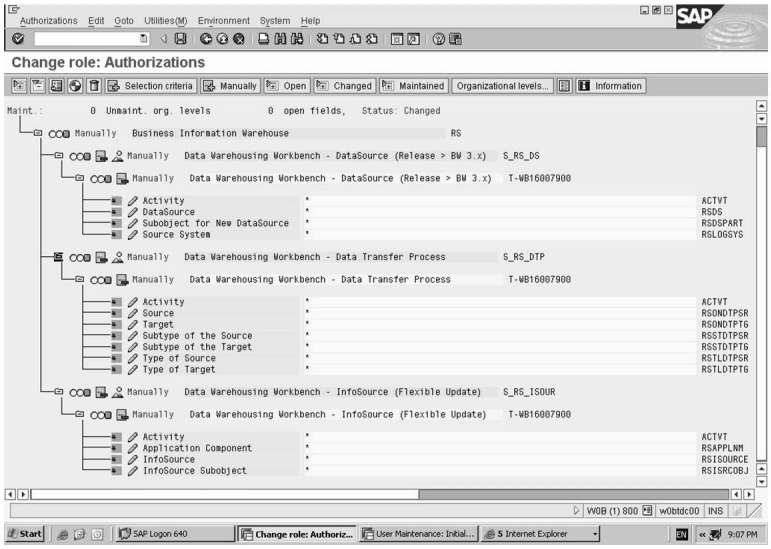


Figure 45: Securing InfoSources and DataSources

S_RS_IOBJ	Authorizations for working with individual InfoObjects and their subobjects .
S_RS_PC	Authorizations for working with process chains
S_RS_OHDEST	Authorizations for working with open hub destinations

Figure 46: Securing Additional DataWarehousing Objects

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Additional DataWarehousing Workbench Objects

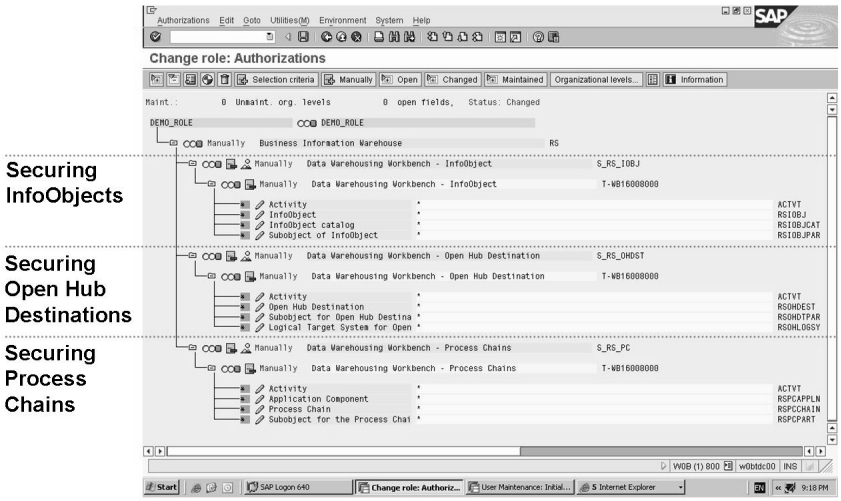


Figure 47: Securing Additional Data Warehousing Objects

Authorization to Remotely Activate Business Content DataSources

The activation of Business Content is an Administrator's task. With the proper authorizations, Administrators may remotely activate the associated source system DataSources during the process of activating Business Content in BI.

This activation is subject to an authorization check: Authorization object S_RO_BCTRA. The authorization is valid for all DataSources of a source system. When the objects are collected, the system checks the authorizations remotely. The system issues a warning if you do not have authorization to activate the DataSources. The activation is done using the <logical system name>_DIALOG RFC destination. There will be a prompt for UserId and PW.

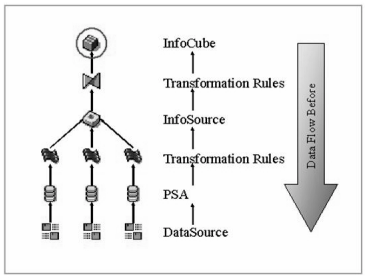
If the user does not have the necessary authorization for activation, the system issues a warning. If the Administrator does not have authorization, the Business Content DataSource will have to be manually replicated and activated.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

- As of NW 2004s BI BCT DataSources are activated remotely in the BI system:
  - Necessary role: SAP_RO_BCTRA
  - Authorization object: S_RO_BCTRA
- D-Versions of BCT DataSources exist in BI after replication of Source System or Application Components (Exception: File DataSources are delivered with BI).
- When grouping BCT Objects for activation the BI system collects in BI the D-Versions of the DataSources.



- During collection, the system already checks the authorizations remotely.
- During activation, the DataSources in the source system are transferred to the active version and replicated in the BI system.
- Depending on the existing Business Content the system decides which DataSource type has to be generated (New DataSource/DataSource 3.x). Activation via transaction RSA6 in the Source System is therefore obsolete now.

Figure 48: Securing Remote Activation of BCT DataSources

Caution: A prerequisite for this feature is that the source system must have BI Service API SAP NetWeaver 2004s (PI_Basis2005.1); otherwise remote activation is not supported. In this case, you have to activate the DataSources in the source system manually and then replicated them to the BI system.

Secure Remote Activation of BCT DataSources

Authorization Object: S_RO_BCTRA

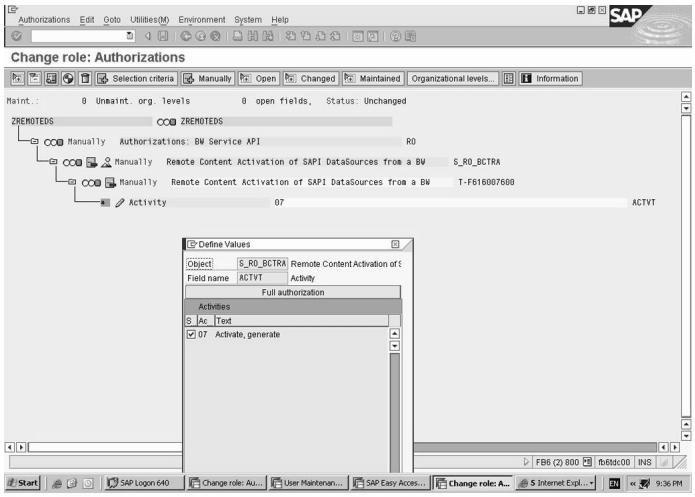


Figure 49: Secure Remote Activation of BCT DataSources

© 2006 SAP AG. All rights reserved.

When a user with the proper authorization activates Business Content with *Grouping* option *Data Flow Before,* the system will check the source system for associated Business Content DataSources and will activate those objects as well. Corresponding Transport Requests will be created on the Source System.

Remote Activation of BCT DataSource

Grouping: Data Flow Before

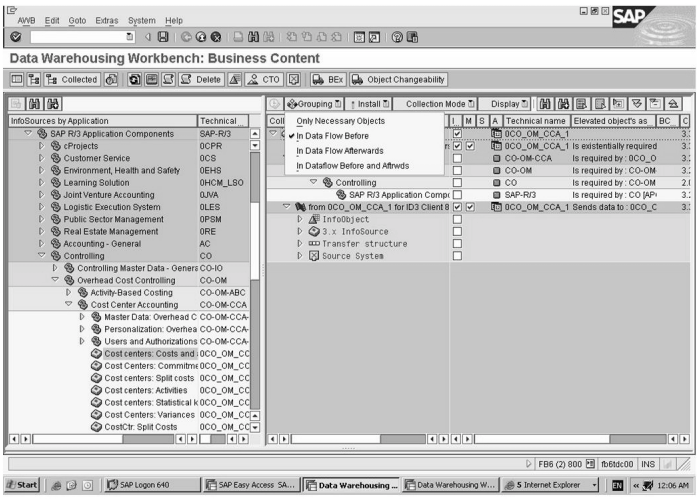


Figure 50: Business Content Activation: Grouping

By choosing *Install,* the activation process is started. A message screen will display, indicating the authorization check is being performed.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Authorization Check for Remote Activation

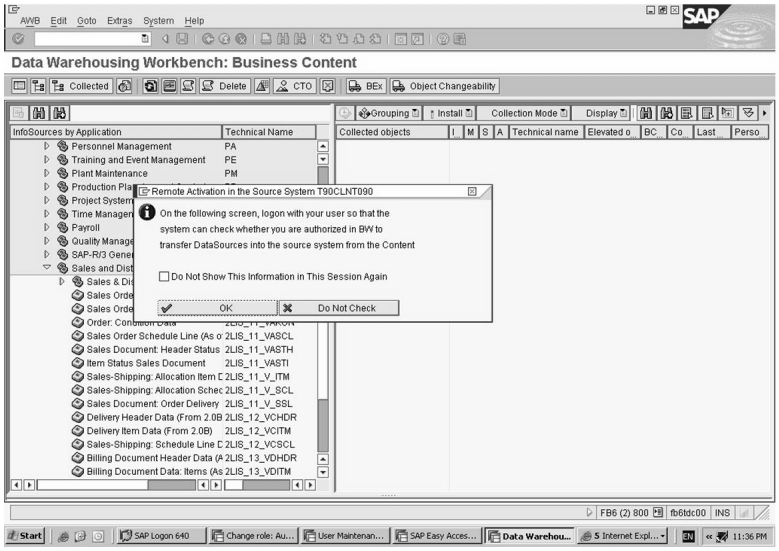


Figure 51: Authorization Check for Remote BCT DataSource Activation

Activated Business Content DataSource

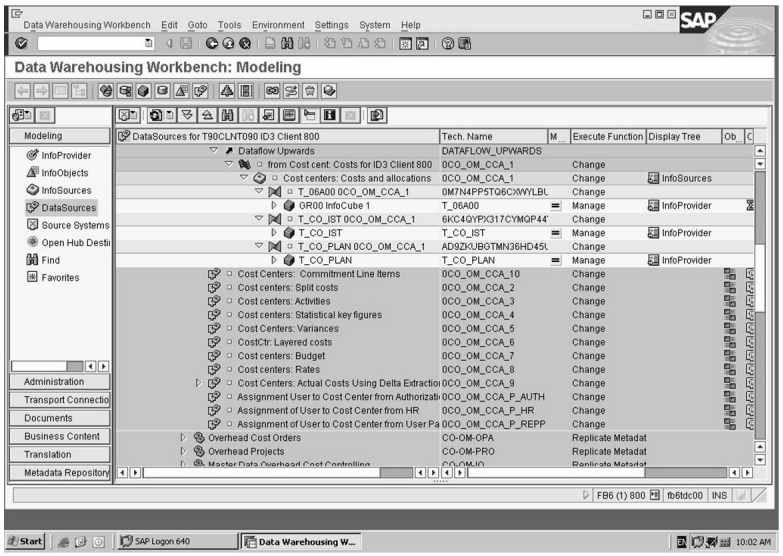


Figure 52: Activated Business Content DataSource

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Securing Master Data and Documents

In order to be able to change or display master data, authorization checks are made. Authorization assignments and checks are defined by characteristic, or by characteristic value.

Master Data Authorization Check

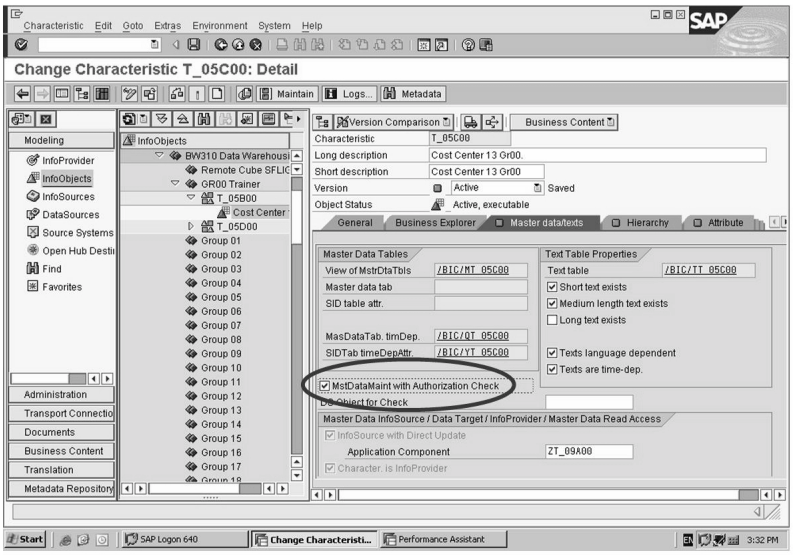


Figure 53: Master Data Authorization Check

To grant authorizations for characteristics, activate authorization assignment by setting Authorization Check indicator in the Master Data/Texts tab page.

The next step is to create a role with the authorizations.

Two authorization objects exist for this:

- S_RS_IOMAD a blanket authorization check takes place for a characteristic.
- S_TABU_LIN an authorization check takes place by characteristic value.

© 2006 SAP AG. All rights reserved.

Role to Secure Master Data Maintenance

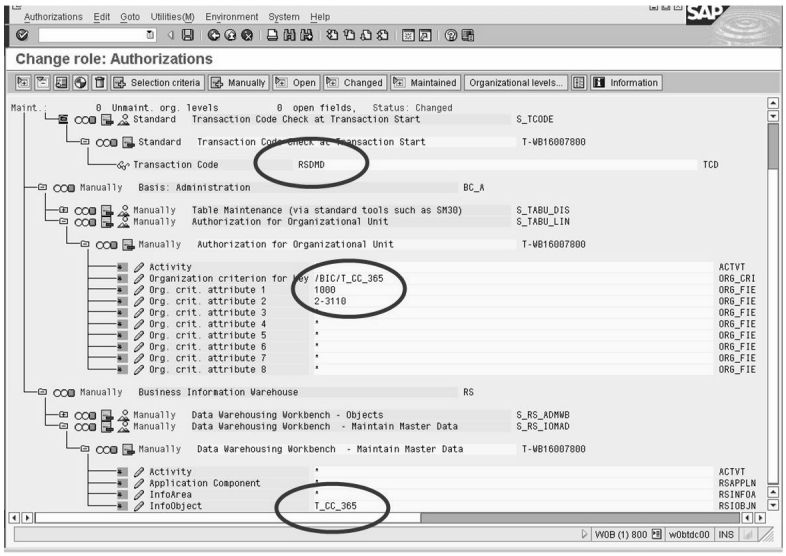


Figure 54: Role to Secure Master Data Maintenance

In Role Maintenance (Transaction PFCG): For blanket authorizations for characteristics, add authorization object S_RS_IOMAD to the role. For authorizations for single characteristic values, add authorization object S_TABU_LIN to the role.

An additional authorization object is needed:

- S_TCODE Transaction code, RSRMD, for master data maintenance.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Master Data Maintenance

Maintenance permitted on these records based on the authorization created in the role.

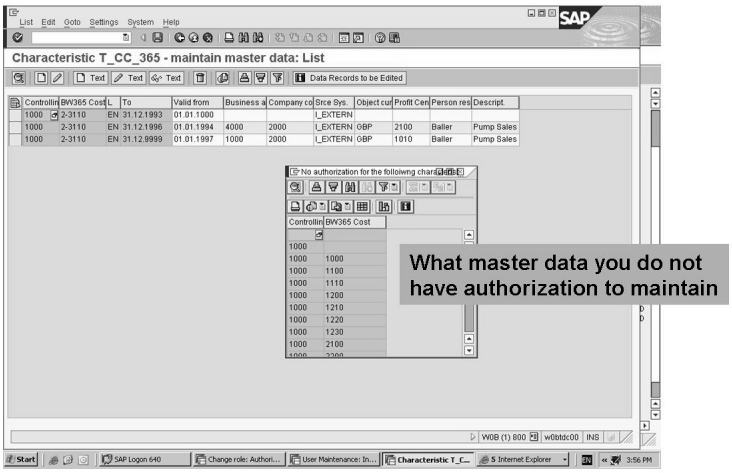


Figure 55: Maintaining Master Data

After user assignment is complete, only the authorized master data can be maintained. In the master data maintenance screen, RSRMD, the user will have access only to authorized master data.

Securing BI Documents

In order to edit documents in the Documents functional area of the Data Warehousing Workbench, the user needs authorization for the authorization object **S_RS_ADMWB**, Data Warehousing Workbench Object, with the following:

- Metadata: DOC_META

  Authorizaton to display or to edit a metadata object, also authorizes the user to display or edit the documents for these metadata objects. Valid activities are: 03 (display), 23 (maintain)

- Master data: DOC_MAST

  Authorization to display or to edit in specific master data, also authorized the user to display or edit the documents for these characteristic values. Valid activities are: 03 (display), 23 (maintain)

- InfoProvider data: DOC_TRAN

  Authorization objects for transaction data, InfoProviders, are not delivered. They are created as required using Analysis Authorizations (RSECADMIN).

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Securing Additional BI Functions

Web Application Designer objects, such as web templates and Web items, can be secured with authorization objects.

S_RS_BTMP	Authorizations for working with BEx Web templates
S_RS_BITM	Authorizations for working with BEx Web items
S_RS_BEXTX	Authorizations for the maintenance of BEx texts

These authorization objects are relevant for managing Web Application Designer Objects: who has access to create, change, display these items

Figure 56: Securing Web Application Designer Objects

S_RS_BTMP protects Web Templates and S_RS_BITM protects Web Items. These authorization objects have three fields: Name, Owner, and Activity.

With the authorization object, S_RS_BEXTX, BEx Texts objects are secured. BEx Texts is a common textpool with language dependent texts maintained via BEx Frontend tools (Web Application Designer and Report Designer).

Authorization Objects for Data Mining

RSDMEMBW	Authorization for uploading data mining results into the BI system
RSDMEMODEL	Authorization for working with analytical models

Figure 57: Securing Data Mining Objects

Each analysis process is only valid for the application for which it was created. The authorizations are also assigned specific to an application and are protected with authorization object RSANPR.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

S_RS_BCS	Authorization for registering broadcast settings for execution.

Special authorizations are required for Information Broadcasting.

- Administrators need authorization object S_RS_ADMWB with the field RSADMWBOBJ = BR_SETTING.
- Users that schedule distribution using Information Broadcasting, require the authorization object S_RS_BCS.

Figure 58: Authoirizations for BEx Broadcasting

The only authorization necessary for the online execution of broadcasting settings is the authorization for the execution of the underlying reporting objects (for example, the Web template). Any user that has authorization to create background jobs also has authorization for direct scheduling in the background. The authorization object S_BTCH_NAM is required for regular scheduling in background jobs.

Securing Process Chains

For the administration processes that are included in a process chain, authorization for authorization object S_RS_ADMWB is required.

S_RS_PC	Authorizations for working with process chains

S_RS_ADMWB is required to maintain the attached processes in a Process Chain.

S_RS_PC is required to maintain the Process Chains.

Figure 59: Securing Process Chains

To create and maintain process chains, authorization for authorization object S_RS_PC is required. This authorization object determines whether process chains can be displayed, changed or executed, and whether logs can be deleted.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Enterprise Portal Logon Methods

SAP EP Supports 2 different logon methods:

- SAP Logon Tickets (SAPLOGONTICKET)
- User ID and Password (UIDPW)

Manual user mapping between EP and BI is required if user ids are not the same.

Single sign on with Certificates and Logon tickets:

- EP Trusts tickets of BI
  - Certificate of EP is imported to BI
- BI Trusts tickets of EP
  - Certificate of BI is imported to EP

Scenarios:

- Call of BI Web Applications from EP
- Publish to EP from Web Application Designer
- BEx Information Broadcasting to EP

Figure 60: BI and Enterprise Portals Logon Methods

From the Enterprise Portal, user mapping is required for two methods of Single Sign-On to backend systems:

- SSO using user ID and password

  in this case, it is necessary to map the portal user ID and password to the user ID and password in the backend system.

- SAP logon tickets for Single Sign-On to SAP Systems

  In this case, users have the same user IDs both in the portal and in ABAP-based SAP systems, there is no need for user mapping. A user's portal user ID and the SAP user ID are stored in the user's SAP logon ticket. When the user tries to access a component system, the system extracts the user ID from the logon ticket (passwords are not sent across networks).

For more information on this topic please refer to the *Security Guide for SAP NetWeaver BI* on http://help.sap.com.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Lesson Summary

You should now be able to:

- Explain how to secure Data Warehousing Workbench objects such as InfoProviders, Data Transfer Processes, DataSources, Open Hub Destinations and Process Chains.
- Describe how to secure remote activation of Business Content DataSources.
- Explain how to protect maintenance of Master Data and Documents.
- Briefly describe how to secure Information Broadcasting distribution and Data Mining Objects.
- List the two logon methods for BI and Enterprise Portals.

Related Information

- See SAP Note 637692 for more information relating to S_TABU_LIN for securing Master Data records.
- See SAP Notes for Logon tickets: 701205, 917950.

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: System Communication Security

Lesson Overview

This lesson will discuss security regarding communication between BI and other systems.

Lesson Objectives

After completing this lesson, you will be able to:

- Explain the required security set up for communication between BI and other systems.
- Explain the RFC destinations required.
- List the profiles used for system communication.

Business Example

As data is being extracted from source systems and transferred into BI, you want to ensure that the data is adequately protected. You need to understand the RFC destinations and how they are affected by security.

System Security Setup

To set up system security, you must set up security for all SAP source systems sending data to BI, in addition to setting up security on BI.

BI Security Setup

In BI, you should create a system (not a dialog) user called **BWREMOTE**. BWREMOTE should have the authorization profile **S_BI-WHM_RFC**.

Note: S_BI-WHM_RFC is a profile, not a role.

This profile will give user BWREMOTE the access needed to extract from an OLTP system. The profile also provides the access required for staging steps to get the data into InfoCubes.

Other SAP Security Set Up

You must set up a user on each SAP system sending data to BI. This includes mySAP ERP, Customer Relationship Management (CRM), Supplier Relationship Management (SRM), Advanced Planning Optimizer (APO), R/3 or any other component SAP system that is sending data to BI.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

On each of these systems, you should create a system user called **BWALEREMOTE**. This user should have the authorization profile **S_BI-WX_RFC**.

Note: S_BI-WX_RFC is a profile, not a role.

This profile will give user BWALEREMOTE the access needed to connect and send data to the BI system.

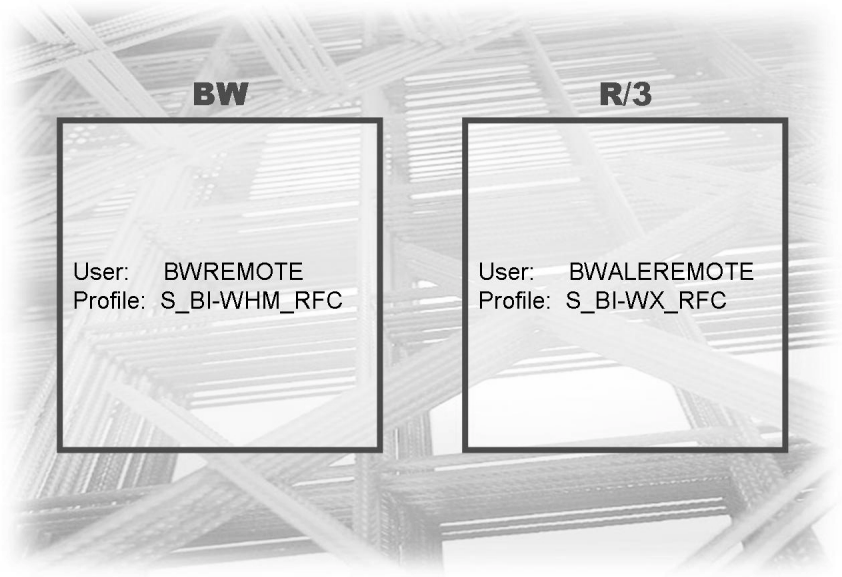


Figure 61: Users for System Communication

It is permissible to use a different name for the users BWREMOTE and BWALEREMOTE. What matters is that the user in BI has the profile S_BI-WHM_RFC and the user in the other SAP system has the profile S_BI-WX_RFC.

RFC Destinations

RFC (Remote Function Call) destinations tell BI where the source systems are physically located. RFC destinations on the SAP source system tell the source system where the BI system is physically located. RFC destinations define where the other systems reside and how to log on to the other systems.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

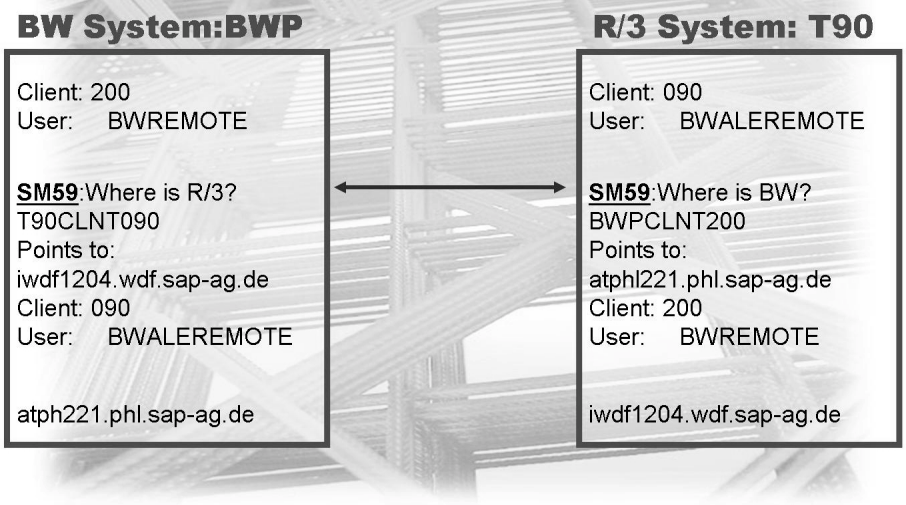


Figure 62: Using RFC Destinations

Setting up RFC destinations is normally not the responsibility of the security administrator. However, the security administrator normally creates the user that is used in the RFC destinations.

The following graphic shows transaction code SM59 on a BI system. This RFC destination is pointing to an SAP system by providing the location of the system and details on how to log on to that system.

Whenever this RFC destination is used, you see BWALEREMOTE, who is logged on to the SAP system. The extraction program that uses the RFC destination has access to all objects to which the user BWALEREMOTE has access.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

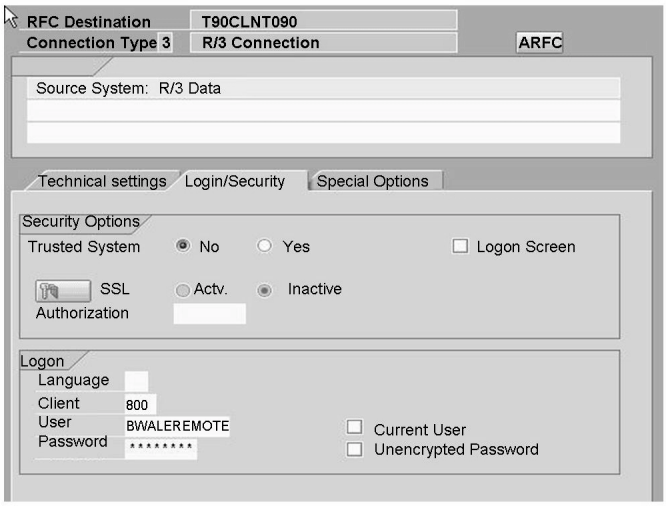


Figure 63: Securing RFC Destinations

Using the <RFC_DESTINATION>_DIALOG Destination

The RFC destination we discussed is used for data extraction. The user IDs involved should be set up as system users. A system user ID cannot log on to a system via a normal GUI screen. The user ID is only for background communication. These user IDs are used exclusively for data extraction processes.

Data extraction, however, is only one of the processes that may require communication between BI and another system. For other system-to-system communication processes in BI, there is another RFC destination defined: the **<RFC_DESTINATION>_DIALOG** destination.

One of the features of BI reporting that relies on system-to-system communication is **Query Drill-Through** (also referred to as jump targets). With Query Drill-Through, the reporting user can select a line on a BI query result and jump to other queries in BI, or even to other reports or transactions in mySAP ERP.

For example, the user may run a BI query showing key figures by material. If configured properly, the user could select a particular material on the report and then ask to jump to mySAP ERP and display the material master record. In this case, BI has to be able to communicate with mySAP ERP in order to log on and execute the transaction code to display the material master record.

Another case where the <RFC_DESTINATION>_DIALOG destination is required involves the monitoring of the data extracted from the source systems. The BI administrator can do this from the BI system.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Status indicators from the extraction process are stored in IDOC format. In the BI *Monitoring* screen, there is an *OLTP* button. This will connect the BI administrator to mySAP ERP so that the administrator can monitor the IDOCS on that system. Whenever the SAP BW administrator selects *OLTP*, the RFC destination <RFC_DESTINATION>_DIALOG is invoked.

The following figure depicts the screen from the monitor function where this RFC destination is being used.

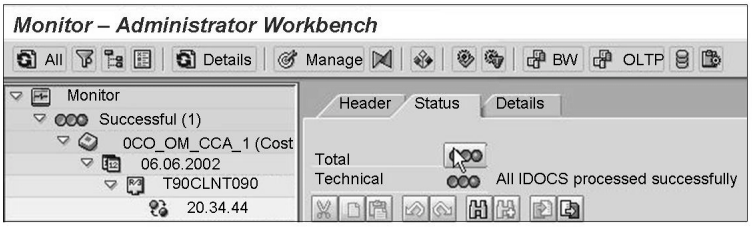


Figure 64: Monitoring IDOCS in BI

When setting up the RFC destination **<RFC_DESTINATION>_DIALOG**, you have some choices regarding the user ID specified:

- Force the user to always log on to mySAP ERP after selecting *OLTP* by leaving the *User* field blank in **<RFC_DESTINATION>_DIALOG**.
- Create a generic user in mySAP ERP with access to monitor IDOCS; use this user in the **<RFC_DESTINATION>_DIALOG** destination.
- In the RFC destination, select *Current User*. This will use the current BI user's user ID to log them on to mySAP ERP.

You must decide how you want the BI user to log on to mySAP ERP from BI to perform the requested task, whether that is jumping from report to report or monitoring the IDOCS generated with data extraction.

If you use *Current User*, the system tries to use the same user ID in BI and mySAP ERP. If this is successful, the BI user can work in mySAP ERP with the usual access rights. If the user ID does not exist in mySAP ERP, then the user will be prompted for a user ID and password.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

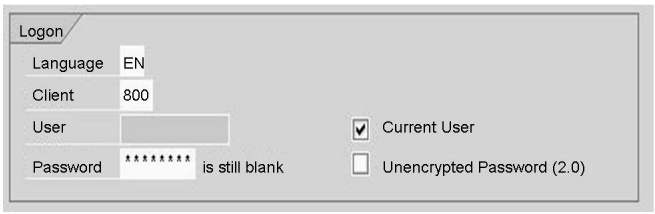


Figure 65: Using *Current User* in _DIALOG Destination

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Exercise 10: Inspect System Communication Setup

Exercise Objectives

After completing this exercise, you will be able to:

- Review RFC destinations
- Review the delivered profiles for system communication

Business Example

SAP BW has been installed and the all the RFC destinations have been configured. You want to make sure that the correct user and profiles are being used.

Task 1:

Look in the RFC destination for logical system T90CLNT090.

1. Execute transaction code SM59. Under *ABAP Connections*, select logical system *T90CLNT090* and answer the questions below.

2. What is the application server for *T90CLNT090*?

   _____
   _____
   _____
   _____

3. What is the user ID used to log on to *T90CLNT090*? How could you check whether the user is defined correctly?

   _____
   _____
   _____
   _____

Task 2:

Ensure that user BWREMOTE on SAP BW has the correct profile assigned.

1. Look at user BWREMOTE and make sure that the profile S_BI-WHM_RFC is assigned.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Solution 10: Inspect System Communication Setup

Task 1:

Look in the RFC destination for logical system T90CLNT090.

1. Execute transaction code SM59. Under *ABAP Connections*, select logical system *T90CLNT090* and answer the questions below.
   a) Execute transaction code SM59.
   b) Expand the *ABAP Connections* portion of the list.
   c) Double-click on logical system *T90CLNT090*.
2. What is the application server for *T90CLNT090*?

   Answer: The application server will be the system listed on the *Technical Settings* tab in the *Target Host* field.
3. What is the user ID used to log on to *T90CLNT090*? How could you check whether the user is defined correctly?

   Answer: The user will be whatever is listed on the *Logon/Security* tab in the *User* field. Most often, this will be user BWALEREMOTE.

   To verify that the user is set up correctly, you would have to look at that user master record via user maintenance or transaction code SU01 in system *T90CLNT090* and verify that the user has the authorization profile S_BI-WX_RFC.

Task 2:

Ensure that user BWREMOTE on SAP BW has the correct profile assigned.

1. Look at user BWREMOTE and make sure that the profile S_BI-WHM_RFC is assigned.
   a) On SAP BW, execute transaction code SU01 and display the user master record for BWREMOTE.
   b) Select the *Profiles* tab and ensure that the user has authorization profile S_BI-WHM_RFC.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Lesson Summary

You should now be able to:

- Explain the required security set up for communication between BI and other systems.
- Explain the RFC destinations required.
- List the profiles used for system communication.

Related Information

SAP Note No. 150315: BW-Authorizations for Remote-User in BW and OLTP

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Unit Summary

You should now be able to:

- Explain how to secure Data Warehousing Workbench objects such as InfoProviders, Data Transfer Processes, DataSources, Open Hub Destinations and Process Chains.
- Describe how to secure remote activation of Business Content DataSources.
- Explain how to protect maintenance of Master Data and Documents.
- Briefly describe how to secure Information Broadcasting distribution and Data Mining Objects.
- List the two logon methods for BI and Enterprise Portals.
- Explain the required security set up for communication between BI and other systems.
- Explain the RFC destinations required.
- List the profiles used for system communication.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Test Your Knowledge

1. Which of the following objects can be secured with S_RS_ADMWB?

   Choose the correct answer(s).

   - □ A Reporting Agent Setting
   - □ B MetaData
   - □ C Web Templates
   - □ D Installation of Business Content
   - □ E Application Components

2. Which of the following authorization objects secures remote activation of Business Content DataSources?

   Choose the correct answer(s).

   - □ A S_RS_ADMWB
   - □ B S_RS_BCTRA
   - □ C S_RS_DS
   - □ D S_RO_BCTRA
   - □ E S_RS_IOMAD

3. The authorization object that secures maintenance for specific master data records or ranges of master data records is:

   Choose the correct answer(s).

   - □ A S_RS_ICUBE
   - □ B S_TABU_LIN
   - □ C S_RS_IOBJ
   - □ D S_RS_IOMAD

4. RFC destinations tell SAP systems where external systems are located.

   Determine whether this statement is true or false.

   - □ True
   - □ False

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

5. Which of the following is a good example of an RFC destination used when the BI administrator monitors IDOCS?

   Choose the correct answer(s).

   - □ A T90CLNT090
   - □ B T90CLNT090_DIALOG
   - □ C T90CLNT090_IDOCS
   - □ D T90CLNT090_R/3_SYSTEM

6. S_MONITOR_IDOC is the SAP-provided profile used by BI to enable communication between BI and a source system.

   Determine whether this statement is true or false.

   - □ True
   - □ False

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Answers

1. Which of the following objects can be secured with S_RS_ADMWB?

   Answer: A, B, D, E

   Web Templates are secure with S_RS_BTMP.

2. Which of the following authorization objects secures remote activation of Business Content DataSources?

   Answer: D

   Remote activation of Business Content DataSources is secured with S_RO_BCTRA.

3. The authorization object that secures maintenance for specific master data records or ranges of master data records is:

   Answer: B

   S_TABU_LIN protects specific data records on master tables. With this authorization, several administrators who have access to the same master data table, would only be able to change records which are specified in their role.

4. RFC destinations tell SAP systems where external systems are located.

   Answer: True

   RFC destinations are used to enable different systems to communicate with each other.

5. Which of the following is a good example of an RFC destination used when the BI administrator monitors IDOCS?

   Answer: B

   The name_DIALOG is used when monitoring IDOCS.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

6. S_MONITOR_IDOC is the SAP-provided profile used by BI to enable communication between BI and a source system.

   Answer: False

   S_MONITOR_IDOC is not a profile provided by SAP.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Unit 6

Maintaining Authorizations

Unit Overview

This unit discusses the various methods of maintaining BI roles and authorizations.

Unit Objectives

After completing this unit, you will be able to:

- Name and evaluate the various maintenance options for authorizations
- Describe how to activate and utilize delivered Business Content roles.
- List the primary templates that are provided by SAP
- Describe how those templates are used
- Integrate templates into roles
- Describe the process of migrating Reporting Authorizations to Analysis Authorizations.
- List and describe the migration methods.
- Explain how to undo a migration.

Unit Contents

Lesson: Maintaining Authorizations 188
Lesson: Using Templates 204
Exercise 11: Using SAP Provided Templates to Build Security for Administrative Users 207
Lesson: Migrating Authorizations 210

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson: Maintaining Authorizations

Lesson Overview

This lesson explains the various options for maintaining authorizations and assigning them to users.

Lesson Objectives

After completing this lesson, you will be able to:

- Name and evaluate the various maintenance options for authorizations
- Describe how to activate and utilize delivered Business Content roles.

Business Example

In your BI system, you have to assign various authorizations for a number of users, mostly in the reporting authorization area. You want to maintain these authorizations as efficiently and clearly as possible.

Reasons for the Various Maintenance Options

- Maintenance of authorizations should be as simple as possible
- The clarity of authorizations should be guaranteed
- The effort required with a high number of users should be as little as possible

The options for authorization maintenance introduced in this lesson – above all the analysis authorizations – function independently of one another. At runtime, it does not matter how the authorizations were assigned to the user. It is only important that the correct authorizations are assigned to the user. In order to maintain the authorizations as simply and clearly as possible, there are various options that you can use independent of the respective authorization scenario. Using the following criteria, you can decide which method is the most appropriate for each.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Criteria for Selecting an Authorization Maintenance Approach

- How large is the number of users?
- Do many users have the same authorizations?
- If the users have different authorizations, do these differ only in the form of individual values?
- Are there many hierarchy authorizations to maintain?
- Is the authorization data available in any form (in another system or in a file)?
- Various security requirements for the maintenance scenarios themselves (example, “dual control principle”)

The Four Options for Authorization Maintenance

The following options for authorization maintenance are available.

Options for Authorization Maintenance

- Role Maintenance
- Analysis Authorization Maintenance
- Customer exit variables for variable authorization assignment
- Generate automatic authorizations

Role Maintenance

Role Maintenance

- Standard
- Correct customizing of roles is important
  - Reusable basic roles separate from more individual roles
  - Menu functions of roles separate from authorizations as needed
  - Avoid overlaps

With role maintenance, we mean classic authorization assignment using roles. This is the recommended standard in cases where it is feasible in regard to required effort. Here you should note that you typically do not create and assign exactly one role per user. Instead, you customize the roles so that are as reusable as possible. A typical example is a role that provides reporting users the basic authorizations to perform reporting. This includes access to the reporting tool, access to the document store in which Web templates or workbooks are stored, and perhaps access to hierarchies or data from InfoCubes (if these are not divided into various areas and thus have to

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

be assigned to various respective users). This type of role can be assigned to every reporting user and the authorizations defined in it do not have to be defined a second time.

Basic Reporting Role Example

These authorizations:

- **Can be assigned to every Reporting User**
- **Do not need to be assigned again in other roles**

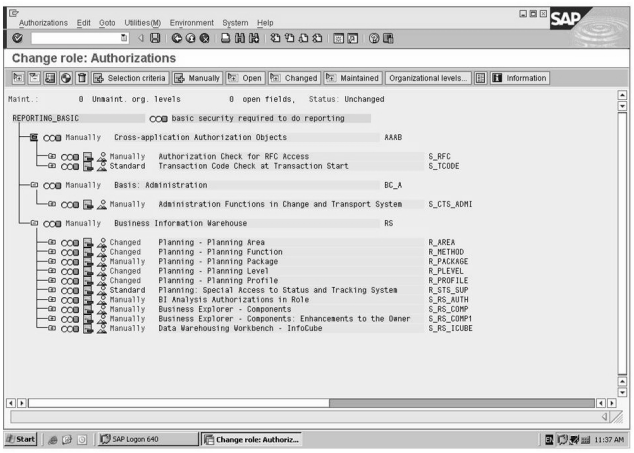


Figure 66: Basic Reporting Role

Often, roles with pure menu functions are separated from roles that include authorizations so that the menus can be used for many users, while different data can be displayed using various authorizations in the queries that are branched to from the menu.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Roles with Menus Only

Menu roles are separated from authorization roles so that:

- **Menus and the attached workbooks can be used by many users**
- **Different results can be displayed based on the user's authorization definitions**

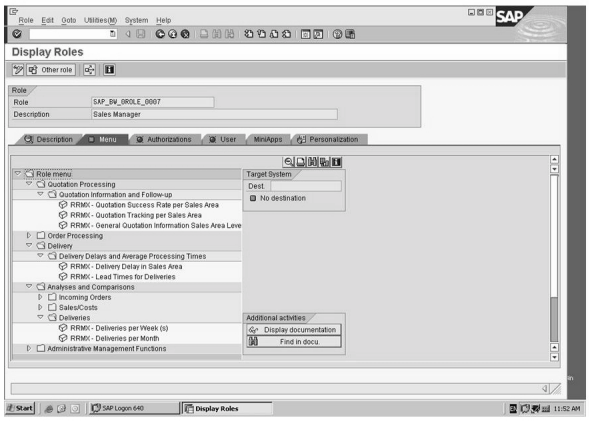


Figure 67: Role with Menu Only

Workbooks are attached to role menus so they can be used by all the users that have that role. Workbooks that are not attached to a role can be identified by executing report RSWB_ROLES_REORG..

Overlapping authorizations between various roles should be avoided as much as possible in order to maintain control and an overview of authorizations. Role maintenance is manual maintenance, where the administrative effort can be quite high in certain circumstances when many users have authorizations that are defined differently. For example, many different authorized values can be required for cost center authorizations. You have to create a role for each value or value combination. To avoid this effort, the methods specific to reporting authorizations described in the following sections can be used. Nevertheless, you will probably use roles that include the basic authorizations and possibly, more easily maintained reporting authorizations that only have a few characteristic values.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Analysis Authorization Maintenance

- All activities for managing the components of **analysis authorizations** are maintained in the Management of Analysis Authorizations transaction, RSECADMIN. (The authorization object S_RSEC protects the analysis authorization maintenance. This authorization object is intended for the assignment of authorizations to the infrastructure of analysis authorizations in the BI-System.)
- In the Management of Analysis Authorizations, analysis authorizations are easily created and maintained. User assignments to analysis authorizations are made quickly from the assign tab. Hierarchy analysis authorizations are created and maintained easily within RSECADMIN.
- With a special authorization object for role connection, S_RS_AUTH, the new analysis authorizations can be assigned using role maintenance.

Assignment of Analysis Authorizations to Roles

Alternatively Analysis Authorizations can be assigned to Roles using the authorization object S_RS_AUTH.

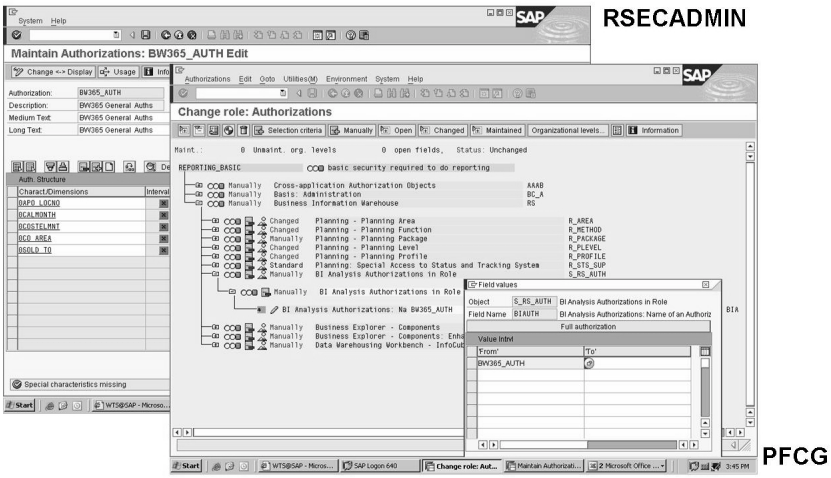


Figure 68: Assignment of Analysis Authorizations to Roles

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

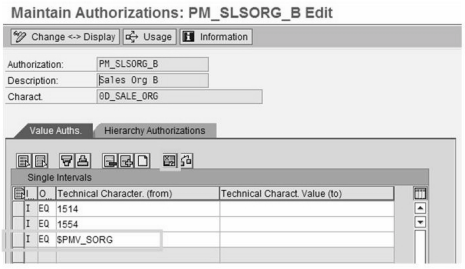
Customer Exit Variables for Authorization Maintenance

- Function of a Variable
  - Normal filtering of queries
  - Hierarchy: determine authorized values
- The authorization assignment via customer exit variables has NOTHING to do with the concept of variables of processing type “authorization”.

The normal function of a variable includes filtering a query with the values with which the variable is filled. A variable of processing type authorization reads the values from authorizations of a user. A variable of processing type customer exit reads the variable values using a selection routine placed in the function module EXIT_SAPLRRBR_001 inside of enhancement RSR0001. (This enhancement is accessed via transaction code CMOD). Both types of variables are primarily used to filter queries. However, you can also use a customer exit processing variable during authorization assignment to achieve a certain amount of flexibility. The variable is evaluated during runtime of the authorization check. However, this logic runs completely independently of the logic used to determine what is filtered in the query and is only used to assign variable assignments. Of course the query should be filtered accordingly or should be able to be filtered accordingly using fixed value restrictions or an input variable, otherwise an authorization error will occur. The same customer exit variable can be used that was used for the assignment. This has the advantage that the authorizations fit exactly to the filter.

Customer Exit Variables for:

- **Hierarchy authorizations**
- **Value authorizations**
  Example: determine sales organization from assignments of the user master data.



$ indicates the variable in the authorization.

Use enhancement RSR00001 (transaction CMOD) for the necessary ABAP coding.

Figure 69: Using Variables for Authorization Values

© 2006 SAP AG. All rights reserved.

The advantage of this method is that you can give all users the same authorization by placing the variable name with a $ sign in front of it instead of a value in the characteristic value (or the hierarchy node).

The variable can also of course be used in the query, but this is not absolutely necessary. You can also filter using another variable or with fixed value restrictions in the query.

Caution: The input length in the authorization is restricted by the number of characters in the underlying characteristic. At the most, the technical name of the variable, including the $ sign, can be doubled by the number of characters in the underlying characteristic by assigning from and to values in the authorization. In the example in the graphic, from $F to DI. This then appears in the upper view as &F to DI.

Automatic Generation of Authorizations

This option for authorization maintenance deals with fully automatic generation. Authorization data is loaded into Data Store Objects and then authorizations are generated with the information from the Data Store Objects.

A prerequisite for this is that authorization data does exist in some form (in a source system) that can be brought into BI with the usual data loading process. The data could come from another SAP system, an external system or a file. With this process, you can avoid duplicate maintenance of data (in the original system and in BI). Here you need to note that due to the various authorization requirements from BI and source systems, mapping is not possible in every case. On the other hand, all the features of transfer and update rules are available to prepare the data so that it can be used for generation.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

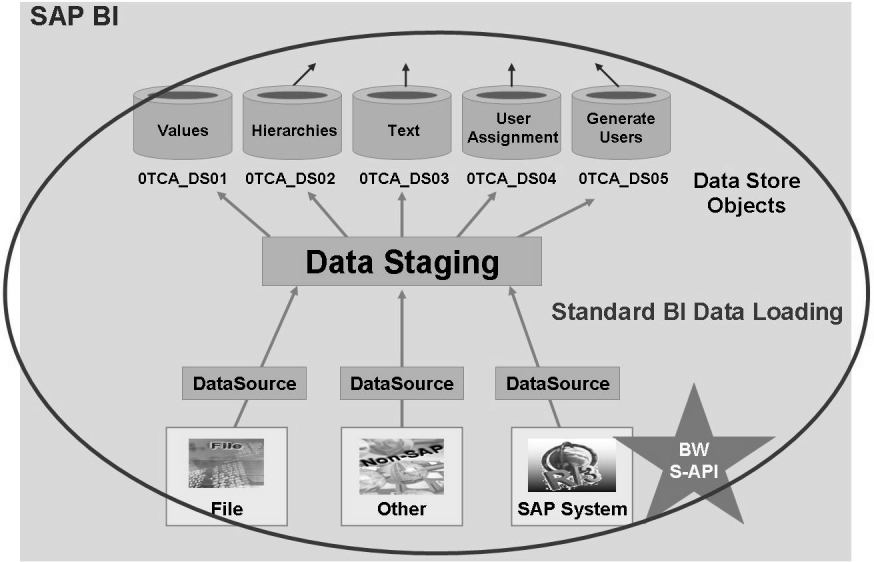


Figure 70: Automatic Generation of Authorizations

There are five Data Store Objects delivered with Business Content that serve as templates:

- 0TCA_DS01 Authorization data - Values
- 0TCA_DS02 Authorization data - Hierarchies
- 0TCA_DS03 Descriptive Text Authorizations
- 0TCA_DS04 Assignment User Authorizations
- 0TCA_DS05 Generate users for Authorizations

For every authorization scenario – typically per authorization object that is to be generated for authorizations – the required DataStore objects should be copied into their own namespace (for example, HR_DS01, HR_DS02,...). In this way, the data for different scenarios is kept separate.

The template 0TCA_DS01 and the copies of it are used for generation of value authorizations (single values, intervals) and 0TCA_DS02 is used for hierarchy authorizations.

Generation of mass authorizations (same authorizations for multiple users) procedure:

Leave the key field *User* empty in Data Store Obtect 0TCA_DS01 and 0TCA_DS02 and generate the authorizations. You then get a profile that can be assigned to any number of users. The profile gets its text from the Data Store Object 0TCA_DS03. You maintain the users in Data Store Object 0TCA_DS04. In this way, you can

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

generate mass authorizations. You can improve the clarity and performance of generation in this way, but usually the first two Data Store Objects are sufficient for having all the functions of authorization assignment. The structure and typical values for these two Data Store Objects can be seen in the figures.

DataStore object for value authorizations (0TCA_DS01)

DataStore Object for Value Authorizations (0TCA_DS01)

InfoObject	Description	Source or value
0TCTUSERNAME	User for which the authorizations is generated	From source data
0TCTAUTH	Technical name of authorization	Initial or name you assigned
0TCTADTO	Validity of the authorization	12.31.9999 or from the source data
0TCTIOBJNM	Name of the authorization-relevant InfoObject	Assignment of source field
0TCTSIGN	Sign	“I” for inclusive
0TCTOPTION	Selection operator	“EQ” – single value “BT” – interval
0TCTLOW	Value or lower interval value	From source data
0TCTHIGH	Upper interval value	From source data
0TCTOBJVERS	InfoObject version	“A” – active
0TCTSYSID	BI System ID	Initial or System ID
0TCTADFROM	Begin of validity	19000101 or source

DataStore object for hierarchy authorizations (0TCA_DS02)

DataStore Object for Hierarchy Authorizations (0TCA_DS02)

InfoObject	Description	Source or value
0TCTUSERNAME	User for which the authorization is generated	From source data
0TCTAUTH	Technical name of authorization	Initial or name you assigned

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

0TCTADTO	Validity of the authorization	12.31.9999 or from the source data
0TCTIOBJNM	Name of the authorization-relevant InfoObject	Assignment of source field
0TCTHIENM	Name of Hierarchy	Constant or from source data
0TCTHIEDATE	Hierarchy key date	Initial or key date
0TCTNIOBJNM	InfoObject of the hierarchy node	“0HIER_NODE” or InfoObject name
0TCTNODE	Account name	From source data
0TCTATYPE	Type of hierarchy authorization	“0”- “4”
0TCTHIEVERS	Hierarchy version	Initial or version
0TCTACOMPM	Area of validity hierarchy authorization	“0” - “3”
0TCTTLEVEL	Hierarchy level	Initial or level
0TCTOBJVERS	InfoObject version	“A” – active
0TCTSYSID	BI System ID	Initial or system ID
0TCTADFROM	Begin of validity	19000101 or source
0TCTNDEF	Default value of node	Initial

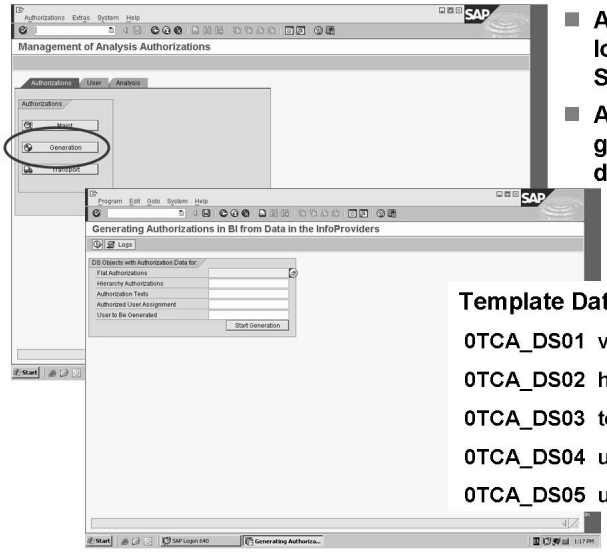
Each data record that is loaded into one of the Data Store Objects includes a value, interval or a hierarchy node for which a user is to be authorized.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Generating Authorizations



- Authorization data is loaded into Data Store Objects.
- Authorizations are generated using the data that was loaded.

Template Data Store Objects:

0TCA_DS01	values (single, intervals)
0TCA_DS02	hierarchy
0TCA_DS03	text
0TCA_DS04	user assignment
0TCA_DS05	user to be generated

Figure 71: Generating Authorizations

For the generation itself, you assign the associated authorization object(s) to the Data Store Objects and then execute them. To automate the generation use transaction RSECADMIN or report RSEC_GENERATE_AUTHORIZATIONS.

A detailed log is created during generation that documents the generation steps.

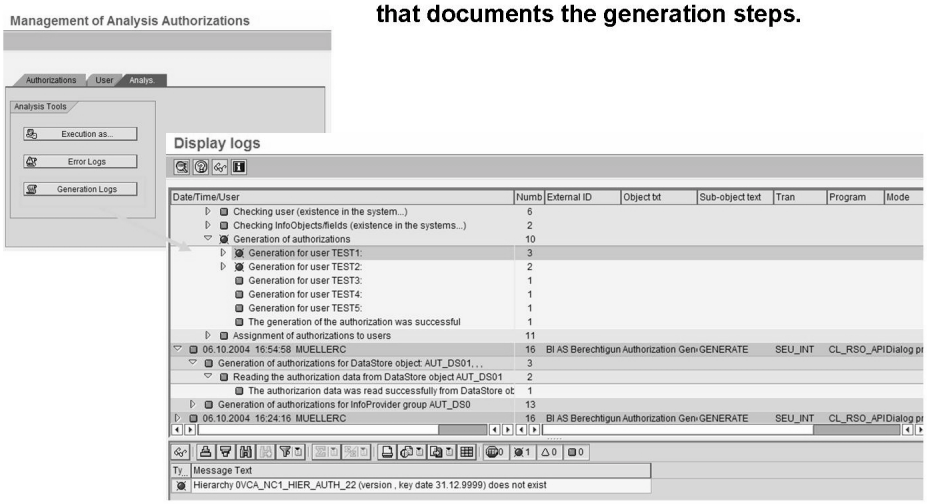


Figure 72: Generation Logs

© 2006 SAP AG. All rights reserved.

A detailed log is created during generation that documents the generation steps. Old logs can be viewed from the transaction RSECADMIN under the *Analysis* tab page, *Generation Logs* or at the start of the report RSEC_GENERATE_AUTHORIZATIONS by clicking on the log symbol.

Properties of the Various Methods

The maintenance method you choose depends on the respective circumstances. The decision can be made using the following characteristics.

Comparison of the various maintenance methods

Comparison of the Various Maintenance Methods

	Efficiency with many users	Clarity	Fulfills security standards	Prerequisites
Role maintenance	- -	+ +	+ + +	none
Analysis Authorizations	+	+++	+++	none
Customer exit	+	+ + +	+ +	Authorization can be derived in the system
Automatic generation	+ +	+	+ +	Authorizations already maintained externally

Business Content

SAP delivered Business Content provides many roles that can be activated and utilized to support a company's authorization strategy. Business Content contains many standard roles as well as roles that were developed for particular industries. Business Content roles can be implemented without being modified or they may serve as templates for building custom-defined roles.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Roles Delivered with Business Content

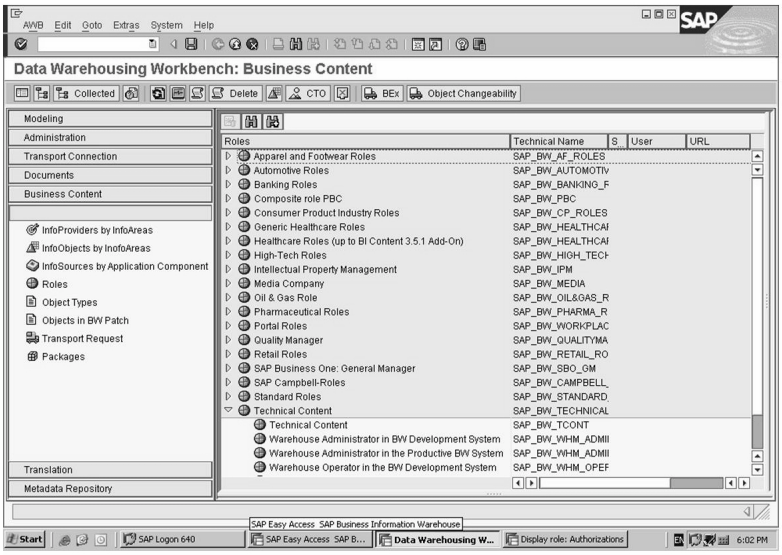


Figure 73: Business Content Roles

Activating Business Content is managed in the Data Warehousing Workbench. By dragging a selected role from the left side to the right side of the Object Collector screen, all the necessary metadata objects associated with the role are grouped together. Grouping options include *'Only necessary objects', 'In data flow before', 'In data flow after' or 'In dataflow before and afterwards'*.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Activating Business Content Roles

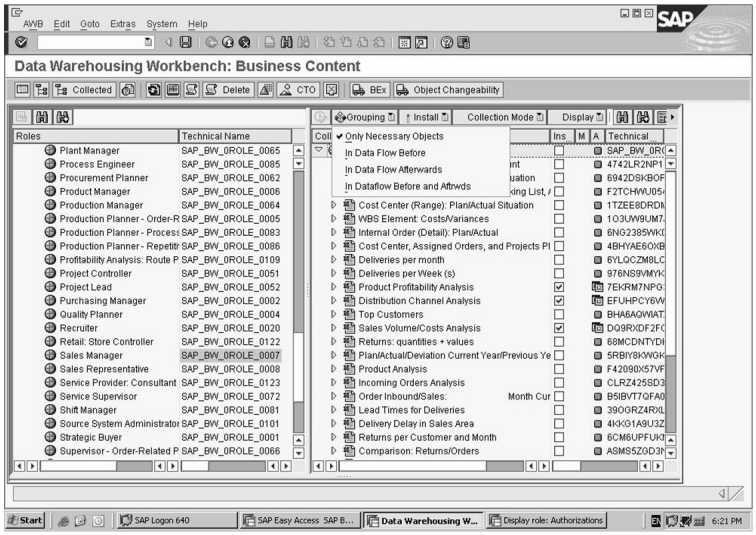
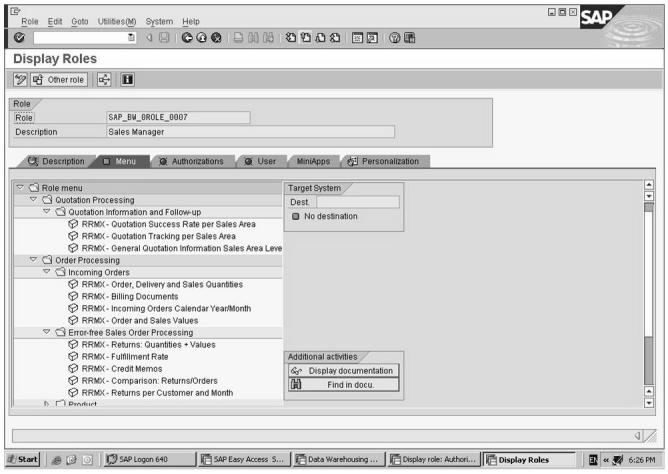


Figure 74: Activating Business Content Roles

Some Business Content Roles have only menus with the attached workbooks, but not authorizations. These roles are typically designed for reporting users.

Business Content Role: Menu Only

This delivered Business Content Role contains a menu with attached workbooks, but no authorizations.



PFCG

Figure 75: Business Content Role with Menu

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Other Business Content Roles may contain user menus as well as authorizations. These types of roles are commonly designed for administrator users.

Business Content Role: Menu and Authorization

This Business Content delivered role contains both a user menu and authorizations.

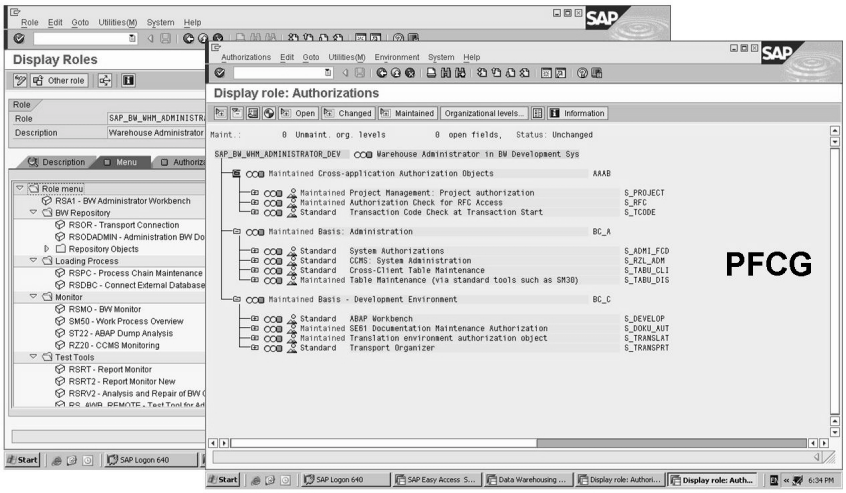


Figure 76: Business Content Role with Menu and Authorizations

The comprehensive list of Business Content roles delivered with BI helps to support a quick and cost-effective implementation. Business Content roles are based on best business practices and therefore also provide excellent guidelines for developing custom roles.

Layering Roles

In BI roles can be managed by InfoAreas, InfoProviders (for example, InfoCubes), reporting components (for example, queries) or InfoObjects. A FI manager in BI may have one role that gives access to specific InfoCubes and another role that gives them access to specific queries or InfoObjects.

For the company using InfoObjects for security, the roles could be similar to how we managed roles in our exercises: one role with basic reporting authorization and another role with specific authorization objects for the sales division and the third role with the workbooks for which an authorization is available.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Name and evaluate the various maintenance options for authorizations
- Describe how to activate and utilize delivered Business Content roles.

Related Information

- Whitepapers on BI authorization are available at http://service.sap.com/bi .

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Using Templates

Lesson Overview

In this lesson, we will discuss the templates provided for building roles for administrators.

Lesson Objectives

After completing this lesson, you will be able to:

- List the primary templates that are provided by SAP
- Describe how those templates are used
- Integrate templates into roles

Business Example

You want to use templates provided by SAP to secure your administrator and power users.

Templates Provided by SAP

Templates enable you to easily insert a set of authorizations into a role. Some companies use templates to support their mySAP ERP authorization strategy, while other companies do not use templates at all. Templates are maintained in transaction code SU24 and used in the *Authorizations* portion of role maintenance (transaction code PFCG).

SAP provides both roles and templates in BI. The roles are mainly focused on reporting users, with most of the provided roles containing SAP-delivered workbooks. SAP also provides templates.

SAP provides many templates to help secure administration users, ranging from users working with the DataWarehousing Workbench, to those maintaining InfoObjects, to reporting developers, to full BI administrators. The following list shows a few of the SAP-provided templates:

- **S_RS_RDEAD**: Administrator on Development System
- **S_RS_ROPAD**: Administrator on Production System
- **S_RS_RREDE**: Reporting Developer on Development System
- **S_RS_TICUM**: Maintain InfoCube
- **S_RS_TICDM**: Maintain InfoCube Data

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Integrating Templates into Roles

After using transaction code SU24 to look at the templates provided by SAP, you might choose to change or create your own templates. After building your templates using transaction code SU24, use role maintenance (transaction code PFCG) to insert the templates into roles.

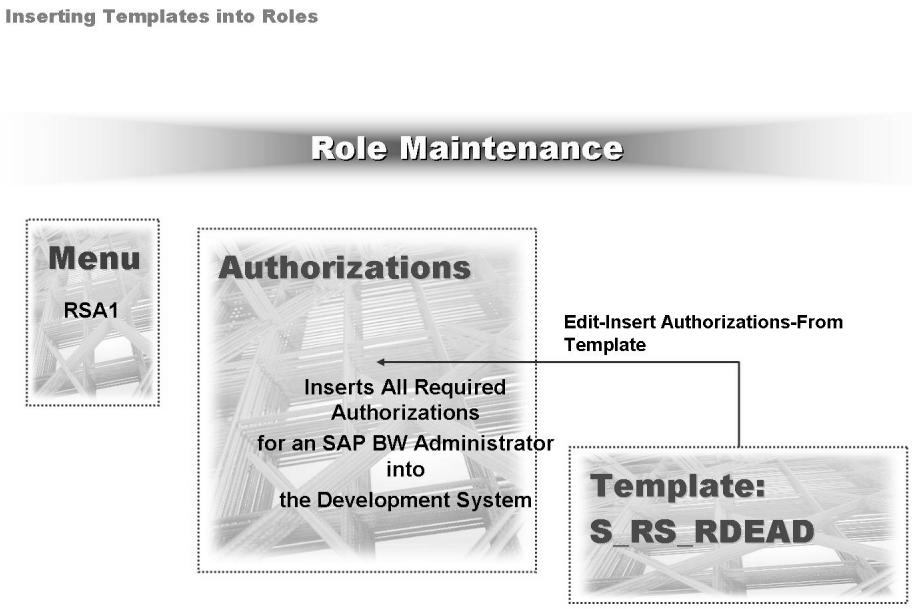


Figure 77: Integrating templates into roles

When building a role that will be used by the BI administrator, the *Menu* area is not highly emphasized. Administrators will be focused on the Data Warehousing Workbench (transaction code RSA1) while query developers will be focused on the BEx Analyzer and Query Designer.

Once you are in the authorization portion of the roles, the *Choose Template* window will appear automatically if the *Menu* is empty. Otherwise, choose *Edit → Insert Authorizations. → From template*, to integrate a template into a role. After inserting the template, you can update, insert, and delete authorizations as needed.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Exercise 11: Using SAP Provided Templates to Build Security for Administrative Users

Exercise Objectives

After completing this exercise, you will be able to:

- Demonstrate the templates that are available for role creation

Business Example

You need to create authorizations for an SAP BW administrator in a development environment and a production environment. You know they will need at least S_RS_ADMWB, but you are not sure of the field values. You want to leverage SAP-provided templates to enable you to create the role more quickly.

Task:

Create a role for an SAP BW administrator on a development system using a template.

1. Use role maintenance to create and save the role **ADMINISTRATOR_##**.
2. In the role definition, select the *Authorizations* tab and insert the template *S_RS_RDEAD BW Role: Administrator (Development System)*
3. There are several authorization object classes inserted from the template. Drill into *Business Information Warehouse → DataWarehousing Workbench - Objects (S_RS_ADMWB)*. Notice the authorizations setup for S_RS_ADMWB.
4. Also look at S_RS_ISOUR and S_RS_ISRCM. What do you notice as a general trend for the authorizations provided in the templates?

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Solution 11: Using SAP Provided Templates to Build Security for Administrative Users

Task:

Create a role for an SAP BW administrator on a development system using a template.

1. Use role maintenance to create and save the role **ADMINISTRATOR_##**.
   a) *SAP menu → Tools→ Administration → User Maintenance →Role Administration→Roles*.
   b) In the *Role* field, enter **`ADMINISTRATOR_##`** and choose *Create Single Role*.
   c) In the *Description* field, enter **`GR## Administrator`**.
   d) Choose *Save* to save the role.
2. In the role definition, select the *Authorizations* tab and insert the template *S_RS_RDEAD BW Role: Administrator (Development System)*
   a) Select the *Authorizations* tab and choose *Change Authorization Data* from the lower part of the screen.
   b) When the list of templates appears, select *S_RS_RDEAD BI Role: Administrator (Development System)* and choose *Adopt reference*.
3. There are several authorization object classes inserted from the template. Drill into *Business Information Warehouse → DataWarehousing Workbench - Objects (S_RS_ADMWB)*. Notice the authorizations setup for S_RS_ADMWB.
   a) Turn on technical names using the path *Utilities → technical names on*.

      Expand object class *Business Information Warehouse*.
   b) Expand the authorization object *Data Warehousing Workbench - Objects*. You will see that all the types of authorizations an administrator needs are set up for you in S_RS_ADMWB. There is an authorization for each action protected by the object, and options for what the administrator needs for that action.
4. Also look at S_RS_ISOUR and S_RS_ISRCM. What do you notice as a general trend for the authorizations provided in the templates?
   a) The activities you need for BI are there, but there is no distinction made between InfoSources or application components. These authorizations will apply to most companies; the only exception would be if you have different BI administrators for different application areas.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- List the primary templates that are provided by SAP
- Describe how those templates are used
- Integrate templates into roles

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Migrating Authorizations

Lesson Overview

In this lesson, participants will learn how to migrate Reporting Authorizations to the new Analysis Authorization concept.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the process of migrating Reporting Authorizations to Analysis Authorizations.
- List and describe the migration methods.
- Explain how to undo a migration.

Business Example

There are Reporting Authorizations that were created in the previous release of BI that you now need to upgrade to the new concept. You would like to migrate the old Reporting Authorization objects to the new concept: Analysis Authorizations.

Migration Tool

	<=SAP NetWeaver 2004	SAP NetWeaver 2004s
Technical Foundation	Authorization Objects	Analysis Authorization
Maintenance	Not Changeable Afterwards	Changeable
Number of objects	10 objects	Number of InfoObjects not limited
Navigational Attributes	Only on global basis	Individually
Hierarchy Authorizations	0TCTAUTHH	Equivalent to value authorizations
Composition of authorizations	Intersection of business objects	Union (as expected)
Authorization Relevance	Per InfoObject AND InfoCube	Only InfoObject setting

Figure 78: Comparing Authorization Concepts

The report RSEC_MIGRATION is available to assist in the migration process. This report supports the manual conversion of old Reporting Authorizations to the new Analysis Authorization concept. These two concepts are very different, so the

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

migration is not a totally complete process. After the migration, the newly created Analysis Authorizations may have to be further edited or partially remodeled. The simpler the original authorization, the less post-migration editing will be required.

Authorization Migration Facts:

Execute Report RSEC_MIGRATION for Migration.

No complete, automatic migration.

- **About 80% automatic migration expected.**
- **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.**

Singular event, not for scheduling.

During migration to the new authorization concept, the existing concept won't be changed.

Figure 79: Authorization Migration Facts

The migration tool, RSEC_MIGRATION, prompts for user, Reporting Authorization object, and method of migration.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

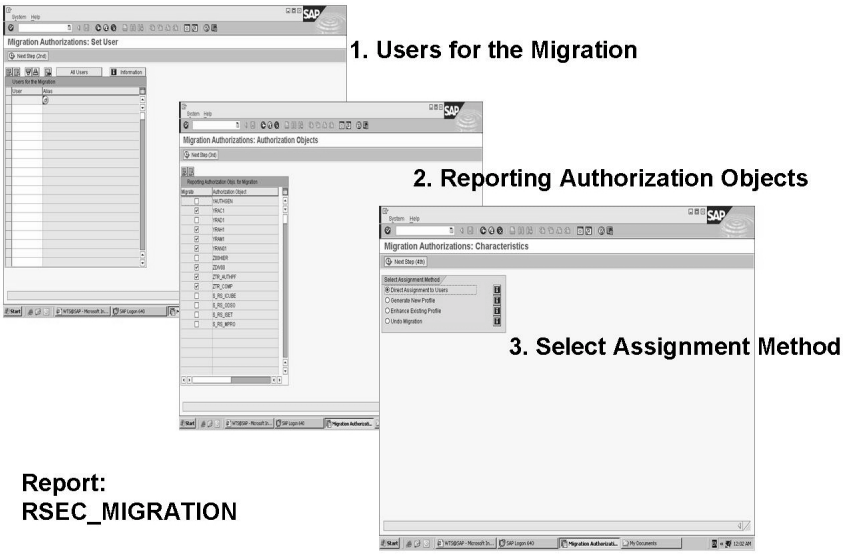


Figure 80: Migrating Reporting Authorization Objects to the New Concept

All users assigned to a Reporting Authorization will be affected by the migration, so only complete user groups can be successfully migrated.

The authorization objects S_RS_ICUBE, S_RS_MPRO, S_RS_ISET AND S_RS_ODSO are no longer checked during query processing. The check is now performed on new Business Content InfoObjects: 0TCAIPROV, 0TCAACTVT AND 0TCAVALID. These InfoObjects are provided during migration, and are generated according to the entries in the InfoProvider and Activity fields from the original authorization.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Migration Methods

- **Direct Assignment**
  - New authorizations assigned to user directly
  - Based on original profile
  - No new profile is created
- **Generation of New Authorization Profiles**
  - New profiles are created
  - A different profile for each authorization
  - Role concept is kept
- **Enhancement of Existing Profiles**
  - Enhances existing profiles
  - New authorizations are added using S_RS_AUTH
  - Profiles are kept as close to originals as possible

Figure 81: Methods for Migrating Authorizations

There are three methods available for migration to the new Analysis Authorization concept. These three methods differ in the type of assignment to the users.

- *Direct Assignment*

  Using this method, authorizations are assigned directly to the users. The assignment is made based on the original profiles, however, no roles or profiles are created during the migration. Use transaction RSU01 to check or change the user and profile assignment if necessary.

  This method corresponds to the assignment of Analysis Authorizations to users in transaction RSECADMIN, Manage Analysis Authorizations. The migrated authorizations appear as generated authorizations in RSECADMIN.

  This method is particularly suitable for smaller installations or for the first simple tests.

- *Generation of New Authorization Profiles*

  With this option, new profiles are created during the migration process. A different profile is generated for every authorization and is then assigned to the users. The generated profile includes an authorization for the new authorization

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

object S_RS_AUTH, with the technical name of the Analysis Authorization as the value. The generated profiles have a technical name that begins with RSR_ and is followed by an 8 digit number.

These profiles are assigned to the same users as the original migrated profile. The role authorization concept is maintained and built parallel to the original. This method easily includes the newly generated Analysis Authorizations into the role concept. After the migration the old authorizations and profiles can be deleted, since they will no longer be needed.

This method is useful if the role concept is maintained. This method is also useful if the old Reporting Authorizations exist in separate profiles that need to be removed after migration.

- *Enhancement of Existing Authorization Profiles*

  This method enhances existing profiles with new Analysis Authorizations using the authorization object S_RS_AUTH. For each Reporting Authorization, a new Analysis Authorization is created and added as a value for the field in S_RS_AUTH, which is then added to the profile.

  Caution:

  When a profile is re-generated in role maintenance, PFCG, the inserted entries from the migration could be deleted. Also, when the migrtion is repeated with another option, the entries are emptied, but the authorization stays the same. In this case, traces of the authorization may remain but do not have any authorization function.

With this option, the role and profile structure can be kept as close to the original structure as possible.

Read the application log that is displayed directly after the program has run in interactive mode. As an alternative, you can go into transaction SLG1 and choose RSEC_BW_AUTH as the object and MIGRATE as the subobject. The log reports success and error events during the migration.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Undoing Migrations

From report RSEC_MIGRATION, choose *Undo Migration*.

All migrated authorizations and profiles will be deleted, extended profiles contain empty authorization object R_RS_AUTH.

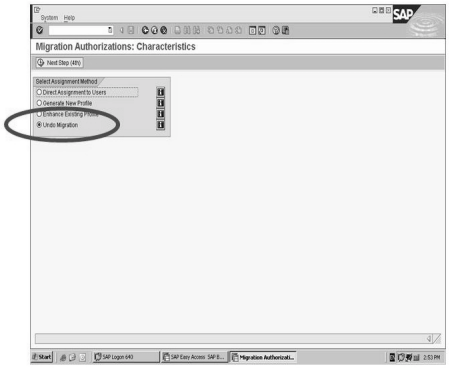


Figure 82: Undo Migration

It is possible, if necessary, to undo the migration, rendering all previous migrations ineffective. The associated generated BI authorizations and profiles are deleted and the entries for authorization object S_RS_AUTH are removed. This step is useful to back out a migration that resulted in a very complicated authorization profile.

To undo a migration, use the *Undo Migration* option in Report RSEC_MIGRATION.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Describe the process of migrating Reporting Authorizations to Analysis Authorizations.
- List and describe the migration methods.
- Explain how to undo a migration.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Unit Summary

You should now be able to:

- Name and evaluate the various maintenance options for authorizations
- Describe how to activate and utilize delivered Business Content roles.
- List the primary templates that are provided by SAP
- Describe how those templates are used
- Integrate templates into roles
- Describe the process of migrating Reporting Authorizations to Analysis Authorizations.
- List and describe the migration methods.
- Explain how to undo a migration.

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Test Your Knowledge

1. SAP provides all the roles you need to secure SAP BW administrators.

   Determine whether this statement is true or false.

   - □ True
   - □ False

2. Which of the following are templates provided by SAP for securing administration users?

   Choose the correct answer(s).

   - □ A S_RS_TICDM
   - □ B S_RS_RDEAD
   - □ C S_RS_ROPAD
   - □ D S_RS_TICUM

3. Use the *Menu* tab in role maintenance to insert templates.

   Determine whether this statement is true or false.

   - □ True
   - □ False

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Answers

1. SAP provides all the roles you need to secure SAP BW administrators.

   Answer: False

   SAP provides templates that you will need to bring into your roles.

2. Which of the following are templates provided by SAP for securing administration users?

   Answer: A, B, C, D

   SAP provides many templates to help secure administration users.

3. Use the *Menu* tab in role maintenance to insert templates.

   Answer: False

   Templates are inserted in the *Authorizations* tab.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Unit 7

Authorizations for Business Planning and Simulation

Unit Overview

This unit describes the security requirements of planning components in BI. In contrast to reporting, in planning, the data of an InfoCube is not just read, it is also changed or created. This results in new authorization aspects. Besides that, the objects for planning have to be secured with authorizations at the same time as other BI objects.

Unit Objectives

After completing this unit, you will be able to:

- Differentiate between Business Planning and Simulation and Integrated Planning in BI.
- Describe the User Interfaces for Planning in BI.
- Explain how planning fits in with BI.
- Describe the special requirements of planning in regard to authorizations.

Unit Contents

Lesson: Planning in BI 222
Lesson: Interaction Between Planning and Other BI Activities 227

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson: Planning in BI

Lesson Overview

This lesson briefly introduces Planning in BI by providing an architectural overview and discussing the BI user interfaces for planning.

Lesson Objectives

After completing this lesson, you will be able to:

- Differentiate between Business Planning and Simulation and Integrated Planning in BI.
- Describe the User Interfaces for Planning in BI.

Business Example

You have been asked to secure BI Planning. In order to do this you now need to understand the basic architecture, terminology and user interfaces.

Planning in BI

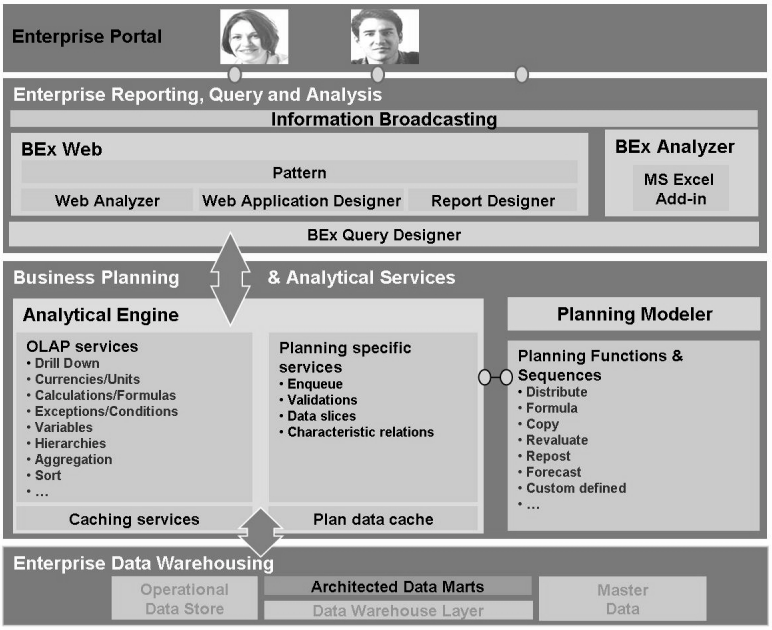


Figure 83: BI Planning Architecture

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

BI Planning allows business experts to accelerate the decision-making process, predict future trends based on historic analyses, uncover hidden or complex relationships between data, and provide all decision makers with a central point of access to data and information.

There are two planning tools in BI:

- BW-BPS (Business Planning and Simulation)
- BI Integrated Planning, a solution that is completely integrated into the BI system.

Business planning is part of the IT scenario Business Planning and Analytical Services.

Both planning tools use the same data basis and can be operated in parallel in one system. It is not necessary to migrate existing planning applications.

Some functions (such as, lock procedure and formulas) are used by both BW-BPS and BI Integrated Planning.

In BI Integrated Planning, most of the BEx and OLAP analysis functions are available for planning applications. In comparison to BW-BPS, you require fewer objects (for example, you use the same variables in analysis and planning) and tools (Query Designer and Web Application Designer).

BW-BPS was the planning tool used in BW 3.5. Integrated planning was introduced with BI NW2004s. Since a large number of BW-BPS concepts are also used in BI Integrated Planning (for example, planning levels, planning functions, planning sequences, characteristic relationships, data slices), switching to BI Integrated Planning from BW-BPS requires a minimal effort.

The Planning Modeler for BW-BPS is transaction **BPS0.**

Use transaction **RSPLAN** to access the Integrated Planning modeler. This transaction links to the web-based tool. A planning wizard is also available for Integrated Planning.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Web Based Planning Modeler

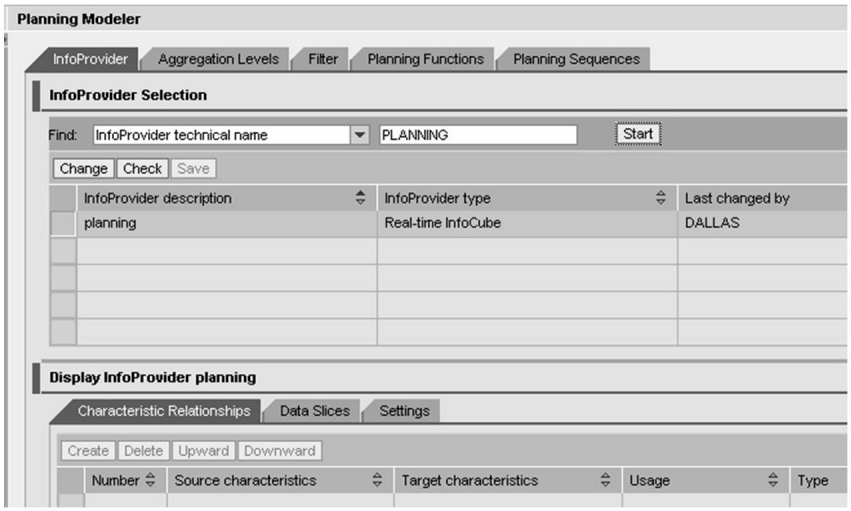


Figure 84: Integrated Planning: Web Based Planning Modeler

The planning modeler is a Web-based application that allows for the creation and modification of any type of planning.

There are delivered authorization templates for Integrated Planning:

- S_RS_PL_ADMIN Planning Administrator
- S_RS_PL_PLANNER Planner
- S_RS_PL_PLANMOD_D Planning Modeler (Development System)

The portal is required to use BI Integrated Planning. A **portal** role is required to use the Planning Modeler: *com.sap.ip.bi.business_planning_showcase.* This role is found in the Portal Content Directory (PCD).

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

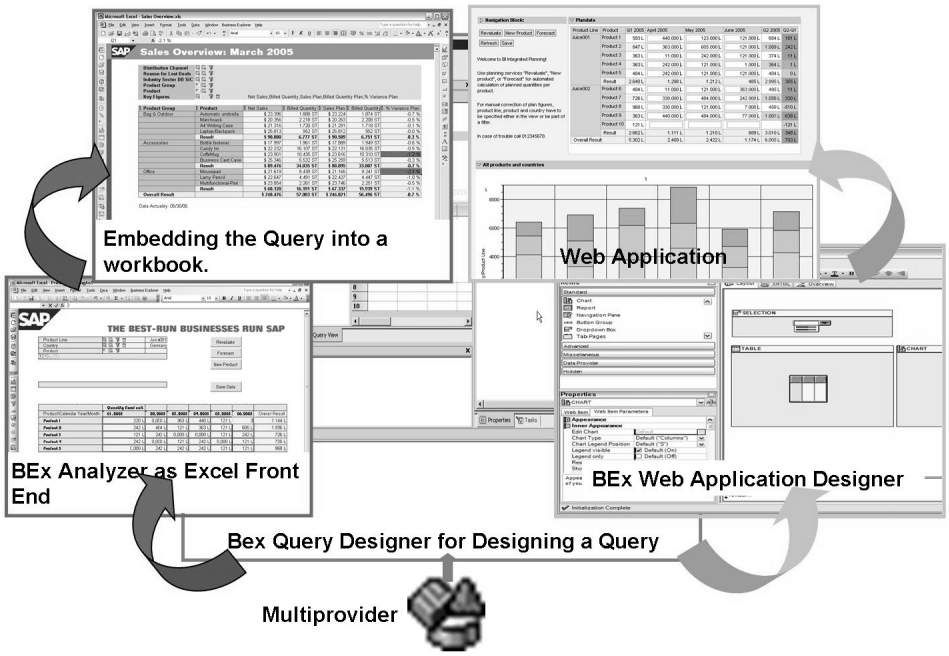


Figure 85: BI Integrated Planning and BEx User Interfaces

In BI integrated planning, most of the BEx and OLAP analysis functions are also available with planning applications.

Both solutions use similar concepts and can be operated in parallel in the system. Unlike BW-BPS, the new solution is completely integrated into the BI system. This allows you to build integrated analytical applications that contain planning and analytical functions. Therefore, we recommend that you use the BI integrated planning structure when you implement new scenarios.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Differentiate between Business Planning and Simulation and Integrated Planning in BI.
- Describe the User Interfaces for Planning in BI.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Lesson: Interaction Between Planning and Other BI Activities

Lesson Overview

This lesson explains how planning fits in with other BI activities with regard to authorizations.

Lesson Objectives

After completing this lesson, you will be able to:

- Explain how planning fits in with BI.
- Describe the special requirements of planning in regard to authorizations.

Business Example

You are already using planning or would like to use planning functions in BI in the future. In order to develop a suitable security concept, all requirements have to be harmonized and taken into account together, including planning.

Planning Concept

- **Plan data can be entered in BI and *Updated* into InfoCubes**
- **On the other hand, the data is also *read* in Reporting (and in the planning process)**

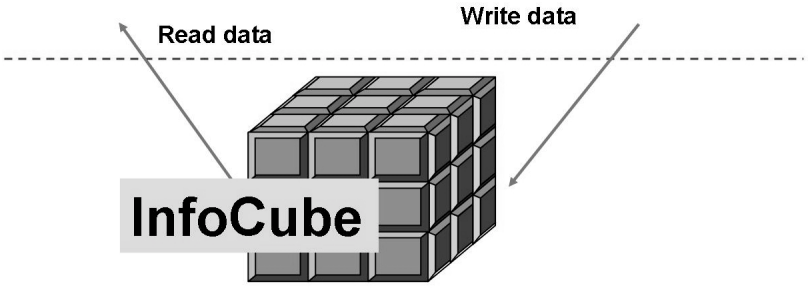


Figure 86: Planning Concept

© 2006 SAP AG. All rights reserved.

In BI there is the option of entering planning data on user interfaces adapted for that purpose and then updating it to InfoCubes, also created for that purpose. For example, budget figures can be planned and written to InfoCubes. These InfoCubes are not (only) supplied with data by scheduled load jobs, but also directly from user entries. Consequently, the technical requirements for the associated objects also change and the requirements for security. There are special planning objects for planning and a special type of InfoCube, real-time InfoCubes. These are set up to deal with a number of small data packages that arrive in parallel. Nevertheless, these are InfoCubes on which reporting can be done, thus the security requirements for reporting and planning overlap. You require authorization from both sides in order to be able to work with the data for the InfoCube.

- **BI authorization objects are checked with planning**
- **Example: Using a query for planning requires authorizations for access to the query (S_RS_COMP) and for the data (analysis authorizations)**

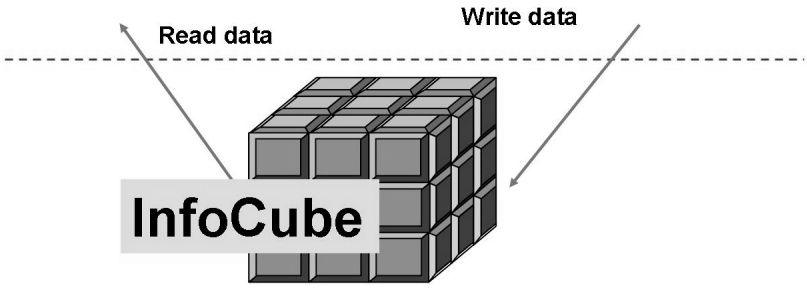


Figure 87: Authorizations for Planning

Reporting Authorization and Planning

The authorizations that users require for BI Integrated Planning are basically the same authorizations they require to analyze the data in a query. In addition to the authorization for displaying data, the authorization for changing data is also required in the analysis authorizations.

The system checks authorization object S_RS_COMP which contains the activity Execute. As InfoProvider you specify the AggregationLevel, MultiProvider or Real-time InfoCube depending on the type of Provider the query or planning function uses.

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

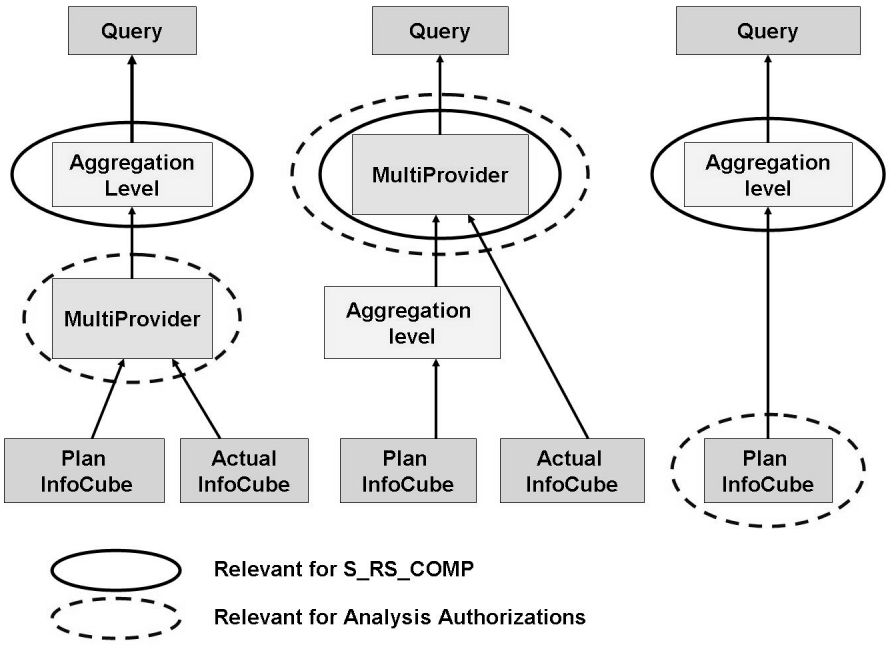


Figure 88: Modeling Options for InfoProviders

The analysis authorizations should not vary from Aggregation Level to Aggregation Level defined on the same InfoProvider. Hence the authorizations are defined for the InfoProvider on which the aggregation level is based. Aggregation levels are transparent as far as analysis authorizations are concerned.

Variables of Type Authorization

Variables are one-dimensional. That's why there is potential mismatch of multi-dimensional selections and automatically filled variables (of type authorization). This is especially relevant with planning because there are typically authorizations on characteristics combined with different acitivities.

Variables of Type Authorization - Typical Situation in Planning

	Country	Activity (0TCAACTVT)
Authorization 1	DE, AT	Display
Authorization 2	CH, DK	Display, Change

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

A variable of type authorization on *country* filters for all countries (*DE,AT,CH,DK*) in the example. If at the same time change authorizations are required for a planning query, the authorization check fails because of missing change authorizations for DE and AT. However, the query would not fail completely but switch to display mode.

The filtering could be refined with a variable of type customer-exit which reads the complete authorization information and filters the *country* based on the activity.

Typical Query: Plan / Actual Comparison

The straight forward approach for a plan / actual query is as follows: The query contains a structure with two elements where the elements contain a key figure and are restricted by version.

Typical Plan / Actual Query - In Line with Authorizations

	Actual Values	Plan Values
	Key figure: 0Amount	Key figure: 0Amount
Material	Version: Actual (display mode)	Version: Plan (change mode)
Material 1		
Material 2		
Material 3		
Material 4		

This definition internally triggers two sub-queries; one for reading the data to be displayed and one for the data to be changed. If the user has authorizations to change plan data and display actual data, this query works for this user.

In the following example the authorization check fails because change authorizations for actual data are checked.

Typical Plan / Actual Query - Authorization Check Fails

		Key figure: 0Amount
Material	Version	(change mode)
Material 1	Actual	

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Material 1	Plan	
Material 2	Actual	
Material 2	Plan	

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Explain how planning fits in with BI.
- Describe the special requirements of planning in regard to authorizations.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Unit Summary

You should now be able to:

- Differentiate between Business Planning and Simulation and Integrated Planning in BI.
- Describe the User Interfaces for Planning in BI.
- Explain how planning fits in with BI.
- Describe the special requirements of planning in regard to authorizations.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Unit 8

Appendices

Unit Overview

We will demonstrate where information can be attained during authorization check runtime.

Unit Objectives

After completing this unit, you will be able to:

- Show the runtime of the authorization check.
- Generate structural authorizations from mySAP ERP HCM in BI

Unit Contents

Lesson: Performance Measurement and Recommendation 236
Lesson: Structural Authorizations BI/mySAP ERP HCM 241

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Performance Measurement and Recommendation

Lesson Overview

We will demonstrate where information can be attained during authorization check runtime.

Lesson Objectives

After completing this lesson, you will be able to:

- Show the runtime of the authorization check.

Business Example

The important things that you need to be aware of are introduced.

After this section, you can describe the major aspects of authorization checks and performance and include them in your design.

Performance Measurement

Authorization Check in BW Statistics

The time for the authorization check is retained in the BW Statistics

In the BW Statistics table:

Data Browser: Tabelle RSDDSTAT

STATUID	TIMEAUTHCHECK
3W8R6CD6YWO64D94RLSG0FIB4	0,179687

BW Statistics query:

Runtime query

Query	Time, authorization check	Time, Read Texts/Master Data
A/0PA_C01_Q006	0,063	0,109
A/0SD_C05_Q0003	0,047	0,000
A/ASYMETRIC4	0,000	0,000
A/ASYMETRIC5	0,016	0,016
A/ASYMETRICCHECK	0,000	0,031
A/BEX_ET_1	0,000	0,047
A/BEX_ET_2	0,031	0,063
A/BW_BEX_ET_QD_RENAM	0,000	0,172
A/BW_BEX_VAR_WIZ	0,000	0,000

Figure 89: Authorization check in BW statistics

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Performance Recommendations

General guideliness for reporting authorizations regarding performance

The most important aspect of authorization performance is designing authorizations and typical query selections in the same way. If the query is typically filtered by single values, then authorizations should also be defined using single values. If intervals or hierarchy nodes are used for selection, the authorizations should be defined in the same way using intervals or hierarchy nodes.

Guidelines for Reporting Authorizations

Reporting authorizations should be defined the same as query selections

Authorizations Selections	Single Value Selections	Interval Selections	Hierarchy Selections
Single Value Authorizations	Usually good, hierarchies may be better when there is a large number of values	Not possible	Not possible
Interval Authorizations	Usually good	Good	Not possible
Hierarchy Authorizations		Not possible	Good

Use * instead of [00000, 99999].

Figure 90: Guidelines for reporting authorizations

The complexity of queries can also play a role. Every selection with a query must be checked for authorizations. The more selections there are, the more complex the check. In some cases, a rough check is enough. For example, it may be sufficient to check only on the InfoProvider level, without having to use reporting authorizations.

Cardinality of authorization checks

The number of authorization checks that take place is affected by the following factors, which also each multiply based on the order of magnitude. Thus the general guideline for keeping the authorization scenario clear is using only the necessary characteristics for authorization checks and using multiple authorization objects (with similar or the

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

same definition) only in exceptional cases. In a large number of authorized values for a user, it is recommended that you consider using full authorization (*) for the user if the requirements allow this.

Influencing factors on number of authorization checks

- Number of authorization-relevant characteristics
- Number of authorized values
- Number of authorization objects
- Scale of authorization checks
- (average # values) x (average # characteristics} x (# authorization objects)

In some cases, the scale of effort required for authorization checks should be even higher, for example when a user has multiple authorizations for an authorization object that cannot be combined into one authorization. This is illustrated graphically in the following image.

Multiple authorizations, not combinable I

- Authorizations that are not combinable require checks on the single value combination level (cartesian product of authorized values)
- Scale of authorization checks
- (# values characteristic 1) x (# values characteristic 2) x …
- Or roughly the same as the formula above:

  (average # values) x (average # characteristics} x (# authorization objects)

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Multiple Authorizations, Not Combinable II

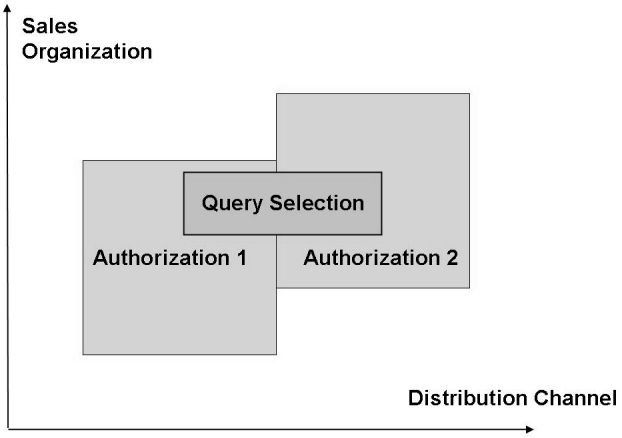


Figure 91: Multiple authorizations, not combinable II

If a performance problem occurs here, you could also consider assigning more authorizations, that is, combining both authorizations into one superordinate authorization if the requirements allow this.

Multiple Authorizations - Enhanced / Combined

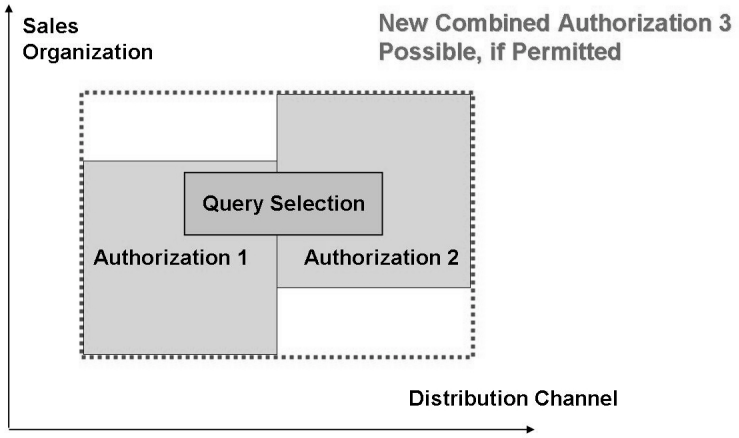


Figure 92: Multiple authorizations - enhanced / combined

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Show the runtime of the authorization check.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Lesson: Structural Authorizations BI/mySAP ERP HCM

Lesson Overview

This lesson deals with the topic of automated authorization generation specific to structural authorizations from mySAP ERP Human Capital Management (old name: *HR*).

Lesson Objectives

After completing this lesson, you will be able to:

- Generate structural authorizations from mySAP ERP HCM in BI

Business Example

You have implemented structural authorizations of the component mySAP ERP HCM in a mySAP ERP source system of BI. You want to use these authorizations in the same way in BI, avoiding duplicate maintenance.

Structural Authorizations in mySAP ERP HCM

Structural authorizations, from a business point of view, have the same function as the general authorizations in mySAP ERP HCM or other SAP components and regulate the access specific to data that is stored in time-dependent structures (organization structures, event hierarchies, qualification catalogs, and so on).

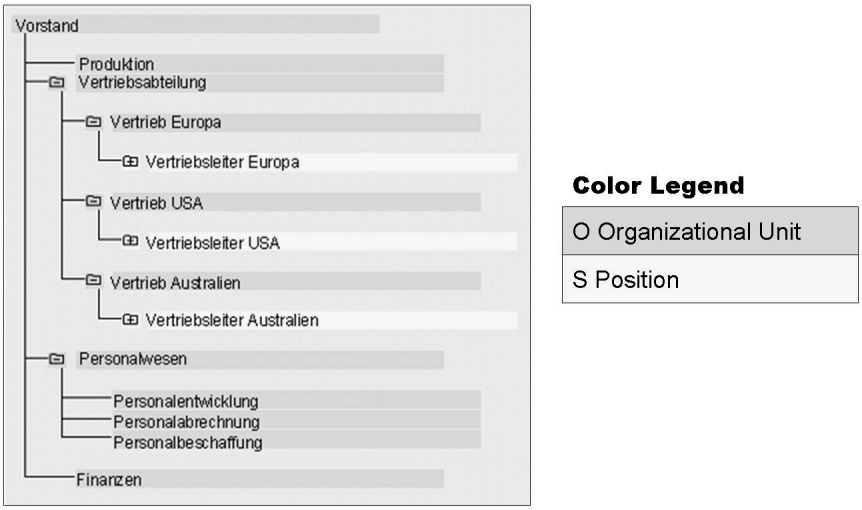


Figure 93: Structural Authorizations - Organization of the Structure

Internal Use SAP Partner Only
Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Prerequisites

The data that you want to protect has to be located in a hierarchical structure of a personnel development component (*organization management, personnel development, event management, etc.*).

Features

Using the structural authorization check, you can assign authorizations for objects that are located within the hierarchical structure and, for example, by specifying a root object you can determine that all objects that are located in the hierarchy under this specific object can be changed. This concept ensures that even when there is a change within the structure, the maintenance effort for structural authorizations will be minimal. At the same time, we can guarantee that users continue to only have access to the objects for which they are responsible. This flexibility is achieved, on the one hand, by using the (initial) structure in organization management to define the authorization profile, and on the other hand, using a concept to store the authorization profile so that the system reacts automatically/dynamically to changes in the organization structure or adapts the various profiles automatically.

Authorizations using organizational structures

- Authorizations are assigned indirectly using organizational structures
  - Organizational Units
  - Job
  - Position
  - Task
- Advantages
  - Maintenance is easier because authorizations are changed accordingly when there are structural changes
  - Clear

Limitation

Structural authorizations are very powerful, thus the following aspects should absolutely be considered:

- In addition to structural authorizations, the general authorizations could also be used, which means mapping the structural authorizations in SAP alone may not be sufficient.
- Authorization requirements in SAP can be different from those in the source system so that the standard mapping of Business Content may not fulfil the requirements.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Procedure

- A prerequisite is that structural authorizations are already created. If not, then these should still be done as part of the mySAP ERP HCM project.
- There are appropriate objects for this in Business Content with which the structural authorizations can be loaded (DataSources, InfoSources, DataStore Objects). These should be activated.
- Scheduling data loading
- Scheduling or manual execution of generation as with the automatic generation scenarios that were already introduced

For structural authorizations, there is special Business Content that includes the entire data flow. Otherwise, it is a generation scenario for DataStore Objects as was already mentioned. An overview of the objects and the data flow can be found in the following figure.

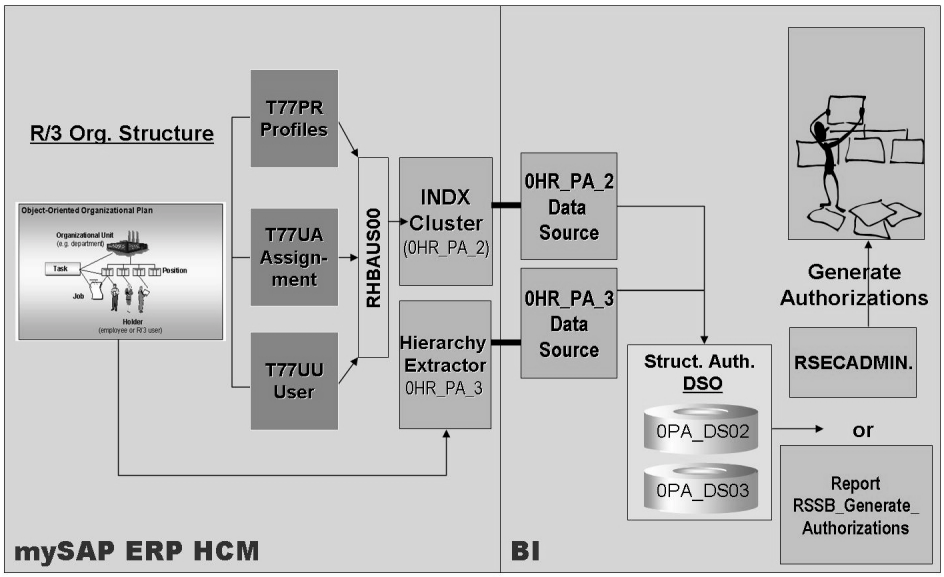


Figure 94: Overview of Data Flow for Structural Authorizations

The following steps are necessary to provide the required data in BI.

- The users for which authorizations were extracted should be entered into the table T77UU (user data are kept in the SAP memory this way)
- Generation of indexes using the report *RHAUS00* in the INDX index cluster

The data can be loaded into the DataStore Objects 0PA_DS02 and 0PA_DS03 using the Business Content data sources 0HR_PA_2 and 0HR_PA_3.

 © 2006 SAP AG. All rights reserved.

Caution: The DataStore Object 0PA_DS02, due to its structure and function, corresponds to the DataStore Object 0TCA_DS01 (the general template for generation of value authorizations) and 0PA_DS03 corresponds to 0TCA_DS02 (hierarchy authorizations).

As for the general case of authorization generation, the following steps must occur:

- the associated characteristics have to have been defined relevant to authorizations in BI for the organization structures (for example 0ORGUNIT).
- the data has to be loaded into the DataStore Objects accordingly.
- the generation for an authorization object that includes the associated authorization relevant characteristics has to take place.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Lesson Summary

You should now be able to:

- Generate structural authorizations from mySAP ERP HCM in BI

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Unit Summary

You should now be able to:

- Show the runtime of the authorization check.
- Generate structural authorizations from mySAP ERP HCM in BI

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Course Summary

You should now be able to:

- Describe BI architecture and how it relates to your security policies.
- Explain the differences and similarities between mySAP ERP security requirements and BI security requirements.
- Secure reporting users, including the authorization objects and authorization values required.
- List the types of tasks required by administration users and describe how to secure those tasks.
- Describe the Business Content roles and templates provided by SAP to assist you in building security for your BI system.
- Explain the security required for systems providing data to BI.

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Glossary

Alert Monitor

A component of the Supply Chain Cockpit that handles common exceptions and problems for all APO applications. The Alert Monitor uses event triggers and alarm conditions established during planning and scheduling to automatically identify problems in the supply chain. It monitors factors such as material, capacity, transportation and storage constraints, as well as metrics such as delivery performance, cost flow and throughput. The Alert Monitor is mainly used by planners to monitor the status of plans in the system. The actual alerts serve as guidelines for future planning.

Application Link Enabling (ALE)

Application Link Enabling (ALE) expands use of SAP R/3 within a company and within a company's business partners. ALE provides software products from SAP distribution models and technologies for linking business applications using technically independent systems. This is possible due to the fact that several database servers use transaction update information simultaneously.

Authorization

Authority to execute a particular action in the SAP system. Each authorization references one authorization object and defines one or more permissible values for each authorization field listed in the authorization object. Authorizations are combined in profiles, which are entered in a user's master record.

Authorization Object

Element of the authorization concept. Authorization objects allow you to define complex authorizations. An authorization object includes up to 10 authorization fields that are checked in an AND relationship. This determines whether a user is allowed to execute a specific action. To pass an authorization test for an object, the user must satisfy the authorization check for each field in the object.

Authorization Profile

Element of the authorization concept. An authorization profile gives users access to the system. A profile contains individual authorizations, which are identified by the authorization name and one or more authorization objects. If a profile is specified in a user master record, the user has all the authorizations defined in this profile.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Business Application Programming Interface (BAPI)
Business Application Programming Interfaces or BAPIs are interfaces within the business framework to link SAPs components to one another and SAP components with third-party components.

Business Content
Predefined information models for processes in SAP R/3 and other SAP applications within the SAP Business Information Warehouse.

Business Explorer (BEx)
This is the reporting tool of the Business Information Warehouse. The Business Explorer consists of the Business Explorer Analyzer and the Business Explorer Browser.

Business Explorer Analyzer (BEx)
A tool in BI that provides reporting on a single ODS Object or on one or many InfoCubes. The BEx also provides Web reporting functions.

Business Explorer Browser (BEx)
With the aid of the BEx Browser you can access workbooks that are assigned to you in channels. You select the workbook with which you wish to work. You manage those workbooks with which you work frequently in your favorites.

Business Framework
Integrated, open, component-based product architecture that encompasses SAP R/3 enterprise applications and third-party products and technologies. The SAP Business Framework provides SAP customers with greatly simplified systems upgrade and maintenance, increased interoperability between R/3, legacy systems, customer-specific and third-party solutions, and a more flexible platform enabling continuous change. The Business Framework evolves to the Internet-Business Framework for mySAP.com.

Business Information Warehouse
New-generation data warehouse used as a basis for making strategic and operational decisions in companies. It combines state-of-the-art warehousing technology with preconfigured business content, and gives users a clear overview of company-internal data and any external data that is relevant. The SAP Business Information Warehouse contains a wide selection of predefined reports that have been specially tailored to meet the needs of specific industry sectors and user groups, e.g. production planners, financial controllers, human resource managers.

Conditions
Terms of payment (such as surcharges or discounts) that are negotiated with a vendor. The conditions determine how the system calculates the net price or effective price.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Currency Translation

Corporate groups must prepare their consolidated financial statements in group currency. Before foreign companies (units in EC-CS/SEM-BCS) can be included in consolidation for the group, their individual financial statements must be translated from local into group currency. The following decisions should be made for the translation: Choice of method: choice between the balance sheet key date exchange rate and the historical exchange rates for the translation of the individual items. Translation differences: Choice between the possible alternatives for handling of translation differences resultin from the translation. Exchange rates: Choice between various exchange rates.

Customer Relationship Management (CRM)

Customer Relationship Management is a set of methodologies, software, and usually Internet capabilities that help an enterprise manage customer relationships in an organized way. It includes all business processes in sales, marketing, and service that touch the customer. For example, an enterprise might build a database about its customers that describes relationships in sufficient detail so that management, salespeople, people providing service, and even the customer can access information, match customer needs with product plans and offerings, remind customers of service requirements, know what other products a customer has purchased, and so on. In contrast to customer care, Customer Relationship Management tends to be used to deal more specifically with the integration of all business functions with each other. SAP also provides applications for Customer Relationship Management under the SAP CRM initiative.

DataStore Object

An object that serves to store consolidated, integrated, and transformed transaction data on a document (or atomic) level. A DataStore Object describes a consolidated dataset from one or more InfoSources. This dataset can be evaluated by a BEx Query or InfoSet Query.

Exception

In an object type component, an error that may occur in the execution of a method and indicates what has gone wrong in the method. Exception categories: Temporary error and Application/system error. Temporary errors may occur when system resources are not available. It may therefore be advisable to call the method again later. You can respond to application or system errors within a workflow by defining steps, which are executed if the exception occurs.

Geocoder

Tool for specifying the latitude and longitude of a location. The geocoder is used to convert address data (for example, Hauptstrasse 150, Heidelberg. Germany.) into exact GEO-coordinates.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Hierarchy

Depiction of a structure that fulfils certain rules. The structure elements of a hierarchy are called nodes. The relationships between the nodes are defined as follows: There is only one top-level node. Only one node is assigned directly above each node (apart from the top level node). Several nodes may be assigned directly below a node. Nodes that do not have any nodes assigned below them are called end nodes. A hierarchy consists of N levels, where N is a positive integer. Assignments directly below or above nodes can exist between neighboring levels only. If a node is on level M (1 < M < N), the node directly above is on level M-1. Any node in a hierarchy that is not the top level node nor an end node represents a sub-hierarchy, together with all the others assigned below it. The node in question is the top level node for this sub-hierarchy.

InfoCube

Multidimensional data model within the SAP Business Information Warehouse to identify, monitor, and analyze key performance indicators.

InfoObject

Business reporting objects (customers, sales,...) are called InfoObjects in BI. They are categorized as characteristics, key figures, units, time characteristics and technical characteristics (for example, request number).

InfoSet

SAP Query element. InfoSets determine to which tables, or fields within a table, a query can refer. InfoSets are usually based on table joins or logical databases.

InfoSet Query

Tool to create lists. Data that is to be available for reports is grouped together in InfoSets. The output medium for the InfoSet Query is the SAP List Viewer.

Key Figures

Quantifiable measure of the technical, commercial and personal performance in a company. Key figures can be used to assess performance, profitability, productivity, and liquidity both within an organization and between one organization and another. Examples: Sales per employee and rate of inventory turnover.

Knowledge Warehouse (KW)

Integrated environment for translation, presentation and administration of multimedia content. The KW has tools and functions to support the company's knowledge management and transfer. With KW SAP training material and the SAP library can be tailored to the company's specific needs.

Metadata Repository

The metadata repository contains the different classes of metadata. With this method of storing and presenting data, a consistent and homogeneous data model results across all source systems.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

MultiCube
A MultiCube brings data from several BasicCubes or RemoteCubes together and places it under one context. The MultiCube itself does not contain any data; its data comes exclusively from the underlying BasicCubes.

mySAP
New SAP solution to integrate all relevant business processes on the Internet. mySAP.com integrates business processes in SAP and non-SAP systems seamlessly, and provides a complete business environment for electronic commerce. mySAP.com comprises four areas: mySAP.com Marketplace, mySAP.com Workplace, mySAP.com Business Scenarios, and Application Hosting.

mySAP Workplace
As part of mySAP.com, the mySAP Workplace represents a role-based and personalized Web browser enterprise portal. The screen is tailored to the specific role of the user in his or her company. Single Sign-On gives the user access to all information, applications, and services that he or she needs for his or her work. The mySAP Workplace provides access to all mySAP.com components, and to non-SAP components and Web services. This includes: All mySAP components, Internet Application Components (IACs), Self-Service scenarios, Reports (such as SAP Business Information Warehouse reports), SAP Knowledge Warehouse content, marketplaces, third-party systems, and any Internet and intranet pages. All in all, the mySAP Workplace provides access to all Web-based systems, applications, and services.

mySAP.com
New SAP solution to integrate all relevant business processes on the Internet. mySAP.com integrates business processes in SAP and non-SAP systems seamlessly, and provides a complete business environment for electronic commerce. mySAP.com comprises four areas: mySAP.com Marketplace, mySAP.com Workplace, mySAP.com Business Scenarios, and Application Hosting.

Navigation
Analysis of the InfoCube data by displaying different views on the data of a query. With the aid of the various navigational functions, such as: 'Fix as filter value' and 'Insert Drilldown According To' you can generate different views of the data (so-called navigational states), that are presented in the results area of the query. Changing views is considered to be navigation. The first view of the data after inserting the query in the workbook is established in the query definition.

OLAP
(OnLine Analytical Processing): Decision support software that allows the user to quickly analyze information that has been summarized into multidimensional views and hierarchies.

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Persistent Staging Area (PSA)

The PSA is the area in BI where transaction and master data from the various source systems are stored initially, without modifications. From the PSA, the transaction data can be loaded either directly to InfoCubes or to the SAP BI ODS. Master data is loaded from PSA into its respective master tables (i.e., master data tables, text data tables, and external hierarchy tables).

Profile Generator

Tool for generating authorization profiles in role maintenance. You use the Profile Generator to generate authorization profiles based on the activities in a role.

Query

Collection of a selection of characteristics and key figures (InfoObjects) for the analysis of the data of an InfoCube or an ODS object. A query always refers exactly to one InfoCube/ODS object, whereas you can define as many queries as you like per InfoCube/ODS object. You define a query by selecting InfoObjects or predefined query templates of an InfoCube/ODS object and distributing them to filters, rows, columns, and free characteristics to create a view of the data. You insert a query in the workbook and can then generate further views of the InfoCube data through navigation. You can save data for the current navigational state of the query in the workbook.

Role

Combination of similar positions. Example: The role “Purchasing Manager” covers the responsibility for orders in the framework of providing basic material, goods and business methods. The task area of the Purchasing Manager entails optimizing the relationship between price and value. Included in the task area of the Purchasing Manager are managing the order process, determining purchasing policies, and procurement market research (process tasks). The Purchasing Manager also plays the role of a superior, that is, he/she supervises the efficiency of the order process, controls the cost center data and is responsible for personnel administration in his/her area (administrative activity functions).

SAP Business Workflow

SAP application component that comprises technologies and tools for automated control and editing of cross-application processes. This primarily involves coordinating: the persons involved, the work steps involved, and the data to be processed (business objects). The main aims are to cut lead times and the costs of business processes, and to improve transparency and quality.

Strategic Enterprise Management (SEM)

Strategic Enterprise Management (SEM) is a suite of tools and processes that managers and executives can use to introduce enterprise-wide, value-chain oriented management practices. SAP SEM provides an integrated, realtime

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

overview of the performance of a company – over and beyond its organizational structures. This enables managers to gauge – and even increase – the value of their company.

Supply Chain Management

Supply Chain Management (SCM): Describes the active management of the entire supply chain from supplier to customer. SAP supports its customers with solutions that integrate information and decisions from the entire supply chain into a seamless, automated, and optimized information infrastructure. It provides the framework for integrating strategic decision support, data warehousing, planning and simulation, forecasting and execution systems in a closed loop with core enterprise financial, logistics and human resource applications. SAP delivers within its Supply Chain Management initiative the applications SAP Advanced Planner and Optimizer and SAP Logistics Execution System.

Template

Dynamic allocation tool that uses functions and formulas to calculate numerical values and the values of Boolean expressions (true or false). This tool is used for various purposes such as sender-receiver allocations and as an aid for formula planning. Instead of preassigned allocation data, the template uses a generic description for any data (such as the sender object, quantities, and costs). Since this data is not known at the time the template allocation is performed, it is determined dynamically when the values are calculated.

Variable

Placeholder used to store and address data under a particular name in a particular format. You can distinguish variables by their name, type, length and structure.

Workbook

File with multiple worksheets (term from Microsoft Excel terminology). You insert one or more queries into the workbook. You can store a workbook in your favorites or assign it to the enterprise catalog. The workbook can then be assigned to one or more channels in the InfoCatalog of the Administrator Workbench.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Index

A

Architected Data Marts
  BI, 4
Authorization
  BI, 9
  InfoObject, 5

B

BI, 3
  Architected Data Marts, 4
  Architecture, 3
  Authorization, 9
  Business Explorer (BEx), 7
  Data Warehouse, 4
  Data Warehousing Workbench, 6, 8
  DataSource, 3
  InfoCube, 7
  InfoPackage, 6
  InfoProvider, 7
  MultiProvider, 7
  Operational Data Store), 5
  Persistent Staging Area (PSA), 4
Business Explorer (BEx), 3
  BI, 7
  Suite, 11
  , *see* Business Explorer

D

Data Transfer Process, 160
Data Warehouse
  BI, 4
Data Warehousing Workbench
  BI, 6, 8
DataSource
  BI, 3

E

Extraction, Transformation, and Loading (ETL), 3
  , *see* Extraction, Transformation, and Loading

I

InfoObject
  Authorization, 5
InfoProvider
  BI, 7

M

MultiProvider
  BI, 7

O

Operational Data Store
  BI, 5

P

Persistent Staging Area (PSA)
  BI, 4

Q

Query Designer, 12

Internal Use SAP Partner Only

 © 2006 SAP AG. All rights reserved.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.

Feedback

SAP AG has made every effort in the preparation of this course to ensure the accuracy and completeness of the materials. If you have any corrections or suggestions for improvement, please record them in the appropriate place in the course evaluation.

Internal Use SAP Partner Only

Internal Use SAP Partner Only

© 2006 SAP AG. All rights reserved.