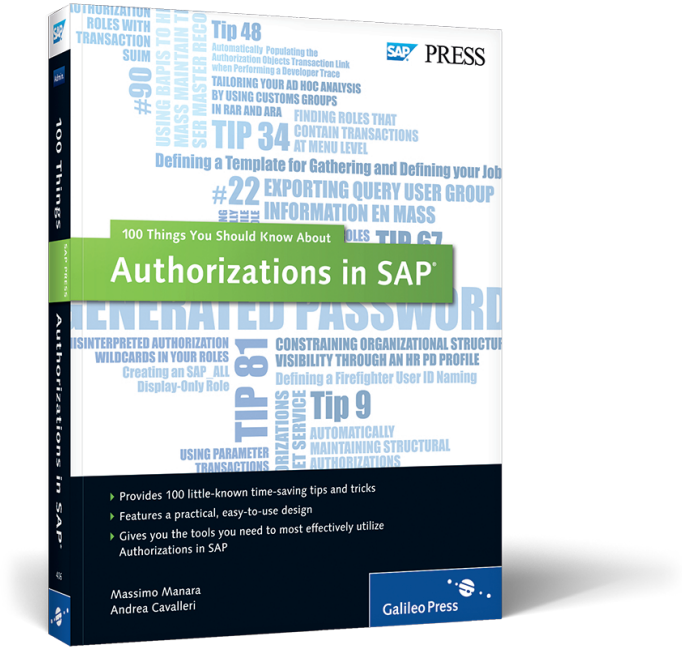
Andrea Cavalleri and Massimo Manara

100 Things You Should Know About
Authorizations in SAP®



Galileo Press®

Bonn • Boston

Contents at a Glance

Contents

Tip 36

Creating an SAP_ALL Display-Only Role

Using Transaction PFCG, you can create a role that provides display-only user access starting with an existing profile.

You should have a wide range of authorization roles to display the system and configuration data in various situations; for example, to assign roles to consultants for a startup and analysis project in development and quality/training systems. You can use Transaction PFCG to create these kinds of roles and ensure display-only access.

And Here's How ...

To create an empty role, access Transaction PFCG (Change Roles), and go to the AUTHORIZATIONS tab (see Figure 1).

The system will ask if you want to use a predefined authorization model. If you want to select a template to fill the AUTHORIZATION tab, choose the SAP_ALL template profile, and then click on ADOPT REFERENCE (Figure 2). In this way, all authorizations entered in the SAP_ALL profile are used to fill up the role.

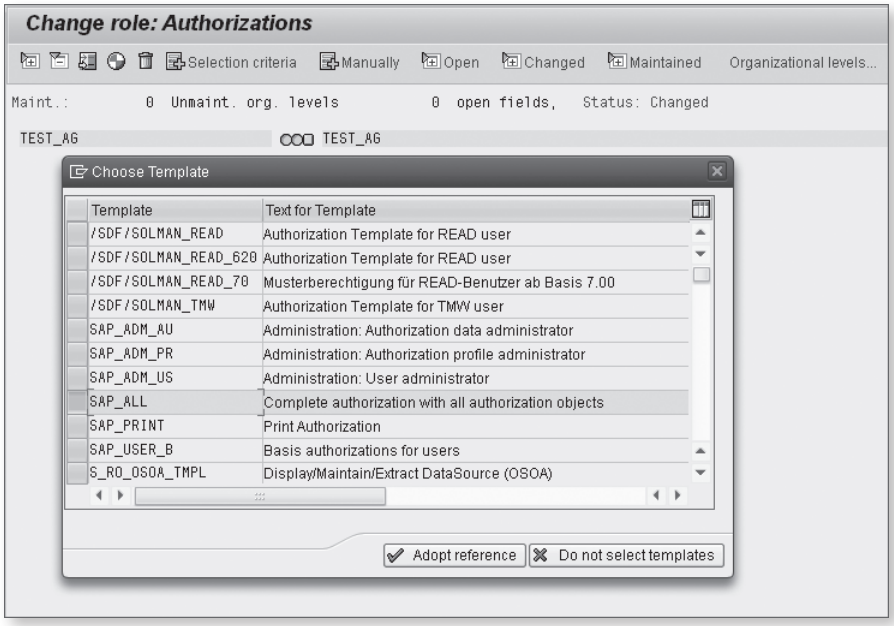


Figure 1 Choose Template Pop-Up Screen

Alternatively, when you are in the authorization tree, you can use the following menu path to enter all authorizations:

EDIT • INSERT AUTHORIZATION(S) • FULL AUTHORIZATION

By doing this, you can ensure that all authorization objects that are entered in the SAP_ALL profile are covered by the role that you are creating.

Next, ensure that this role lets the user access the system in display mode only. Use Table TACT to discover all possible activity entries for the ACTVT field. Common display activity codes are 03 (display), 04 (print), 08 (display changes documents), and 09 (display prices). Activity codes 27, 28, 29, 53, and 54 display activities mainly used in the Controlling (CO) module; 33 reads on the file system directory. Be sure that in all authorization objects with the ACTVT field, the values chosen are in display.

Look for all authorization object fields with the ACTVT field, and set them in display mode by entering the previously listed values (see Figure 2). To do this, click on the binoculars icon, and then find all authorization objects with the ACTVT field.

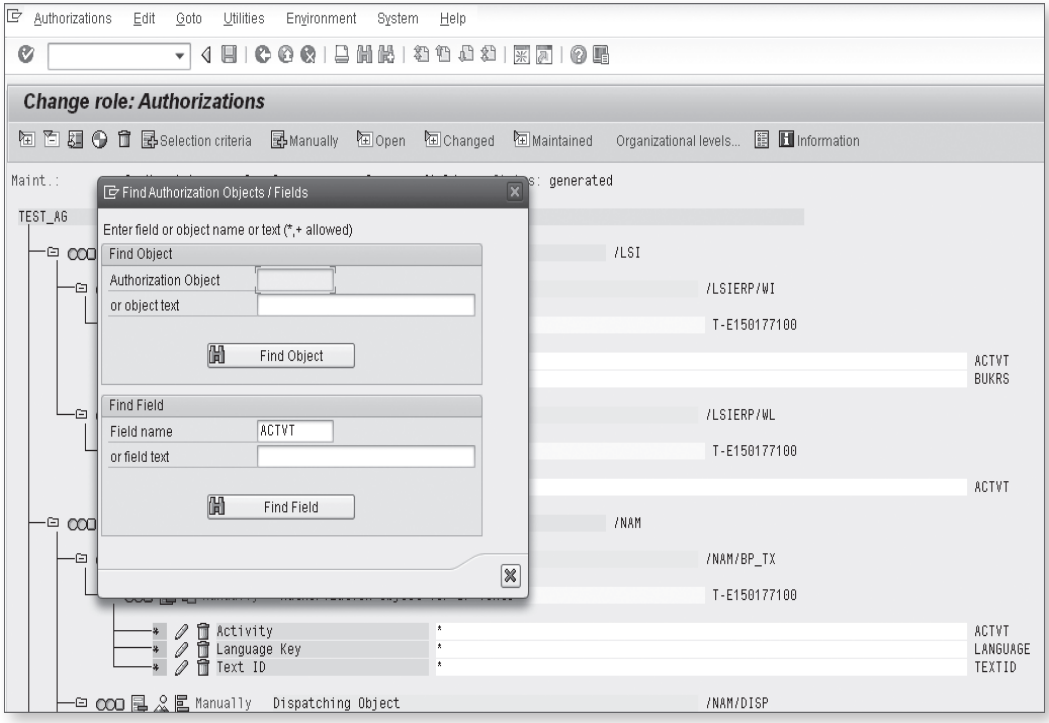


Figure 2 Display Authorizations with the ACTVT Field

If the ACTVT values entered are only in write mode for a certain authorization object, you have to deactivate the object. This is time consuming but is a one-time process. At the end of this setup activity, check whether all values are properly deactivated by accessing Transaction SE16 and browsing Table AGR_1251. Enter your role name in the AGR_NAME field, enter the value "ACTVT" in the FIELD field, and exclude all display values previously listed (03, 04, 08, etc.) in the LOW field. The query in Figure 3 shows you all of the authorization objects where ACTVT is not in the display mode values.

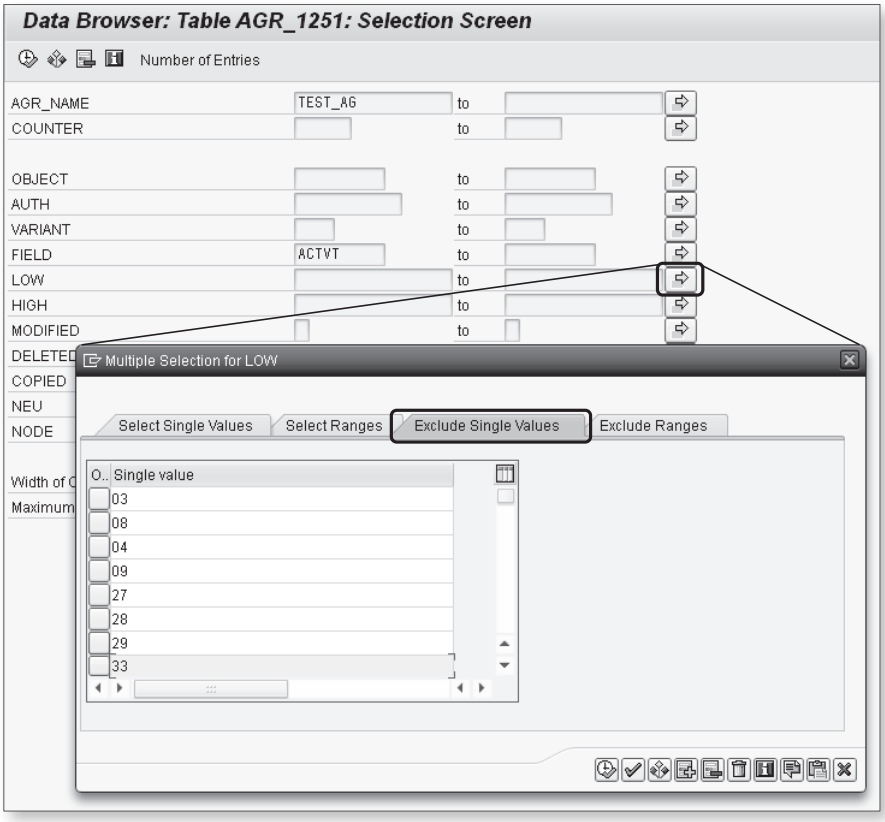


Figure 3 Browsing Table AGR_1251 with Transaction SE16

Note that not all authorization objects have an ACTVT field for managing the activity; in the HR component, the ACTVT field is AUTHC, where the value "R" means read mode. It's also a good approach to disable all authorization objects that are critical, based on your internal policy for your company. You can also limit transaction execution by entering a range in `S_TCODE` authorization objects (e.g., if this role should be allowed to run all transaction except Transaction PFCG). Keep in mind that a range approach can decrease governance because it's more difficult to document the roles and be aware of what the roles allow.

Tip 41

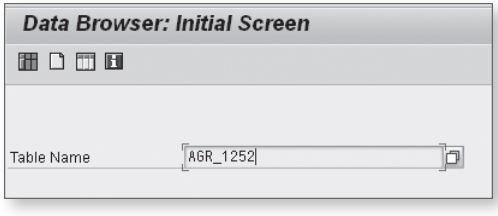
Finding Misinterpreted Authorization Wildcards in Your Roles

You can find wildcard values in your roles by browsing SAP tables and using Microsoft Excel or Access to export your results.

You can use wildcard characters in authorization values. However, if an authorization value contains other characters after an asterisk, the SAP kernel ignores these characters during the authorization check. For example, the value A*B* is actually interpreted as A*. You can find these cases quickly by browsing SAP tables and exporting your findings for analysis through Microsoft Excel or Access.

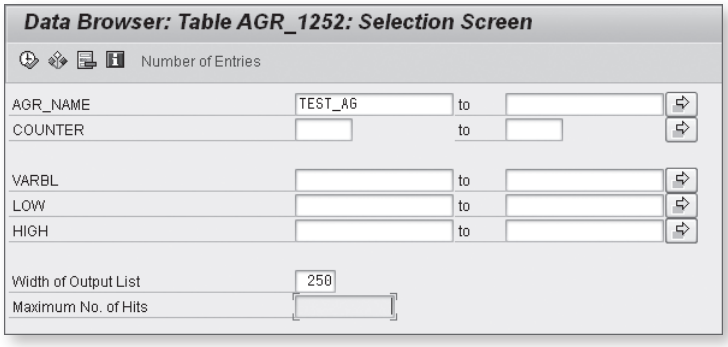
And Here's How ...

Through Transaction SE16, you can directly browse SAP tables that contain the authorization objects and values of a role (shown in Figure 1). You can also browse Tables AGR_1251 or AGR_1252. This example shows you how to find which authorization values in your system contain wildcards that have not properly been set up via Table AGR_1252, which contains the organizational authorization level values for a role. Fill in the TABLE NAME field and press Enter.



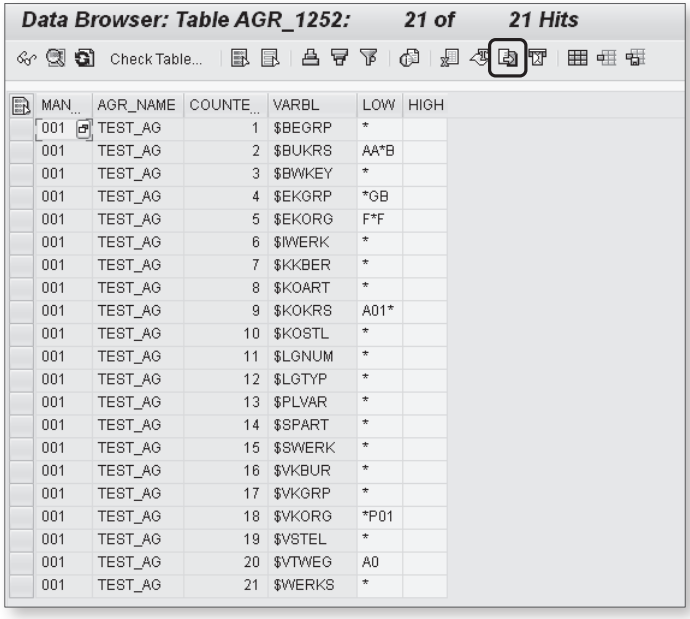
« *Figure 1 Execute Transaction SE16 on Table AGR_1252*

In the selection screen interface (see Figure 2), enter your role name in the AGR_NAME field and press F8.



« *Figure 2*
Transaction SE16 Selection Screen

As a result, you can see all authorization organization values in this role (see Figure 3).

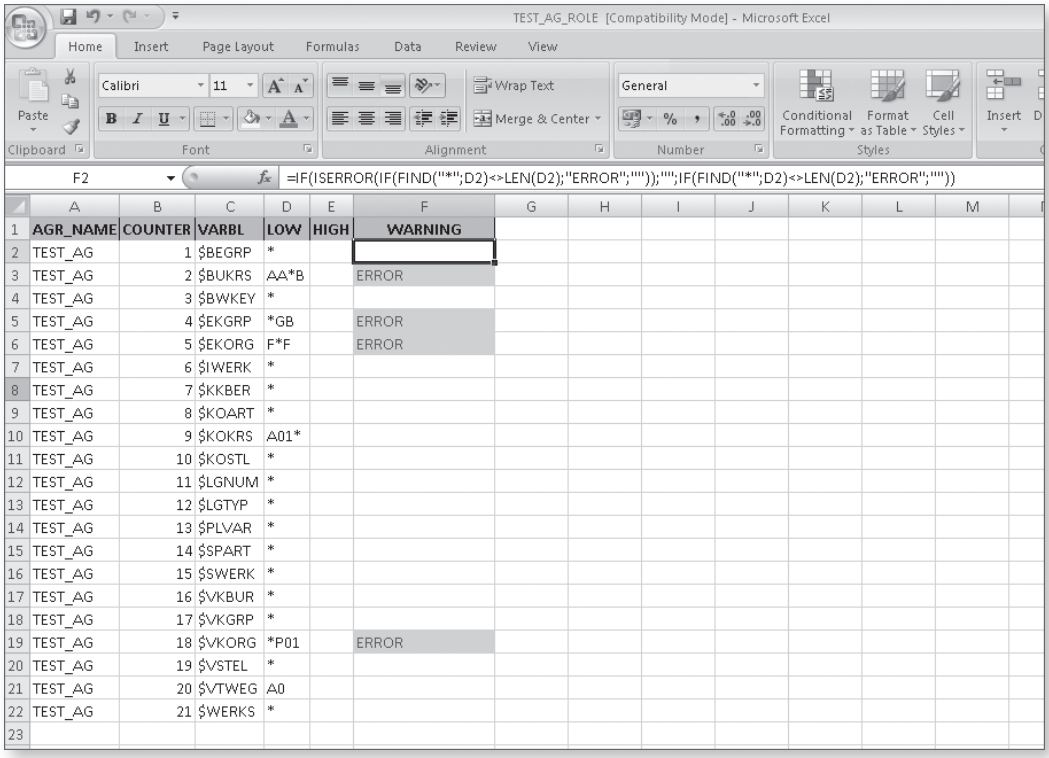


MAN...	AGR_NAME	COUNTE...	VARBL	LOW	HIGH
001	TEST_AG	1	$BEGRP	*	
001	TEST_AG	2	$BUKRS	AA*B	
001	TEST_AG	3	$BWKEY	*	
001	TEST_AG	4	$EKGRP	*GB	
001	TEST_AG	5	$EKORG	F*F	
001	TEST_AG	6	$IWERK	*	
001	TEST_AG	7	$KKBER	*	
001	TEST_AG	8	$KOART	*	
001	TEST_AG	9	$KOKRS	A01*	
001	TEST_AG	10	$KOSTL	*	
001	TEST_AG	11	$LGNUM	*	
001	TEST_AG	12	$LGTYP	*	
001	TEST_AG	13	$PLVAR	*	
001	TEST_AG	14	$SPART	*	
001	TEST_AG	15	$SWERK	*	
001	TEST_AG	16	$VKBUR	*	
001	TEST_AG	17	$VKGRP	*	
001	TEST_AG	18	$VKORG	*P01	
001	TEST_AG	19	$VSTEL	*	
001	TEST_AG	20	$VTWEG	A0	
001	TEST_AG	21	$WERKS	*	

« *Figure 3*
Organization Authorization Values in Role TEST_AG and the Local File

Export this table into an Excel spreadsheet by clicking on the Local File icon circled in Figure 3, and then choosing the Spreadsheet checkbox. Use a formula (such as "`=IF(ISERROR(IF(FIND("*";D2)<>LEN(D2);"ERROR";"")));"";IF(FIND("*`

”;D2)<>LEN(D2);”ERROR”;””))”) to find the misinterpretation of these values from the SAP kernel (see Figure 4).



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	AGR_NAME	COUNTER	VARBL	LOW	HIGH	WARNING							
2	TEST_AG	1	$BEGRP	*									
3	TEST_AG	2	$BUKRS	AA*B		ERROR							
4	TEST_AG	3	$BWKEY	*									
5	TEST_AG	4	$EKGRP	*GB		ERROR							
6	TEST_AG	5	$EKORG	F*F		ERROR							
7	TEST_AG	6	$IWERK	*									
8	TEST_AG	7	$KKBER	*									
9	TEST_AG	8	$KOART	*									
10	TEST_AG	9	$KOKRS	A01*									
11	TEST_AG	10	$KOSTL	*									
12	TEST_AG	11	$LGNUM	*									
13	TEST_AG	12	$LGTYP	*									
14	TEST_AG	13	$PLVAR	*									
15	TEST_AG	14	$SPART	*									
16	TEST_AG	15	$SWERK	*									
17	TEST_AG	16	$VKBUR	*									
18	TEST_AG	17	$VKGRP	*									
19	TEST_AG	18	$VKORG	*P01		ERROR							
20	TEST_AG	19	$VSTEL	*									
21	TEST_AG	20	$VTWEG	A0									
22	TEST_AG	21	$WERKS	*									
23													

Figure 4 Discover SAP Kernel Misinterpretation

In this manner, you can quickly find these misinterpretations on several thousands of roles and fix them.

Tip 44

Troubleshooting Authorization Problems for Users

As an administrator, you can monitor and analyze an authorization problem during a user session with Transaction ST01.

In normal cases, when a user receives an authorization error, the end user or administrator will execute Transaction SU53; this transaction shows that the last authorization check failed. However, you'll find that this error log isn't sufficient to resolve the problem when working with custom or standard transactions. In these cases, you'll find it necessary to perform an authorization trace during a user session with Transaction ST01.

And Here's How ...

To place a trace on a user, execute Transaction ST01 and flag the AUTHORIZATION CHECK indicator under the TRACE COMPONENTS box (❶). Click on the GENERAL FILTERS button (❷), and enter the user ID in the TRACE FOR USER ONLY field (❸, see Figure 1).

After setting Transaction ST01 filters, click on the TRACE ON button. From this moment until you click on TRACE OFF, all activities performed by the user MMANARA are logged depending on your earlier settings (in this case, only whether the authorization check passed and failed).

After the user completes the test session and after you terminate the trace, you can analyze the activities performed by the trace by clicking on the ANALYSIS button. The system shows you the analysis filter selections (see Figure 2) where you have to enter the test user ID and type F8.

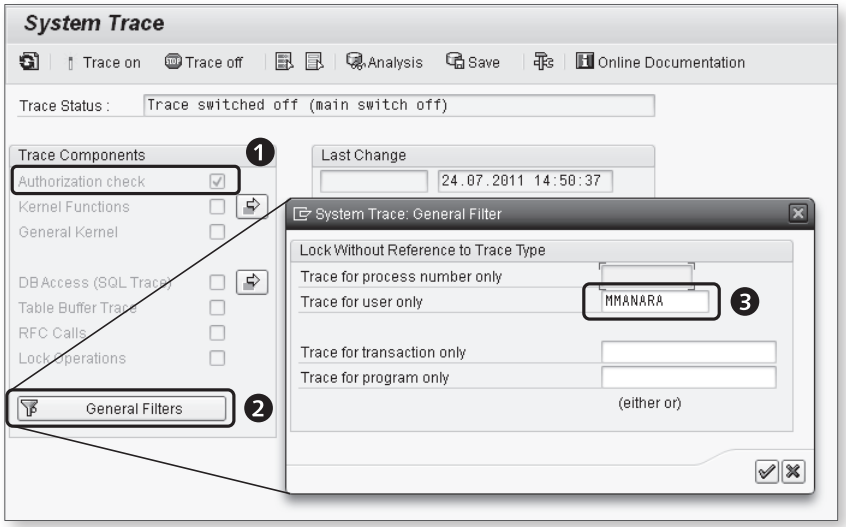


Figure 1 Setting Up Transaction ST01 Filters

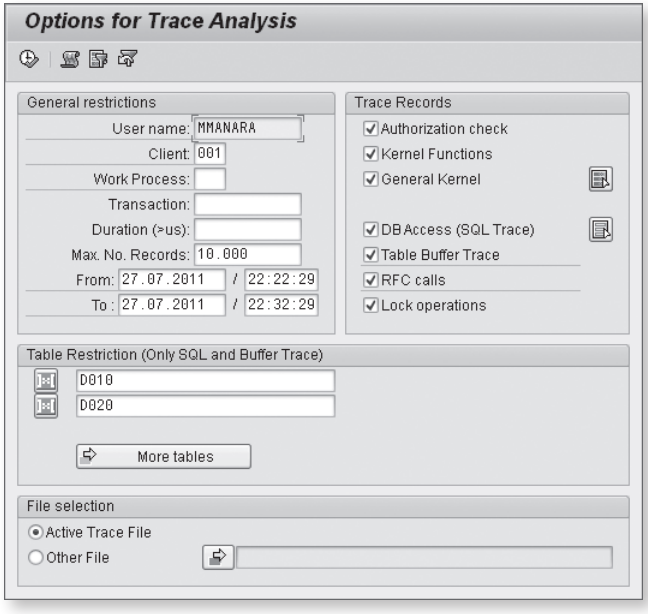
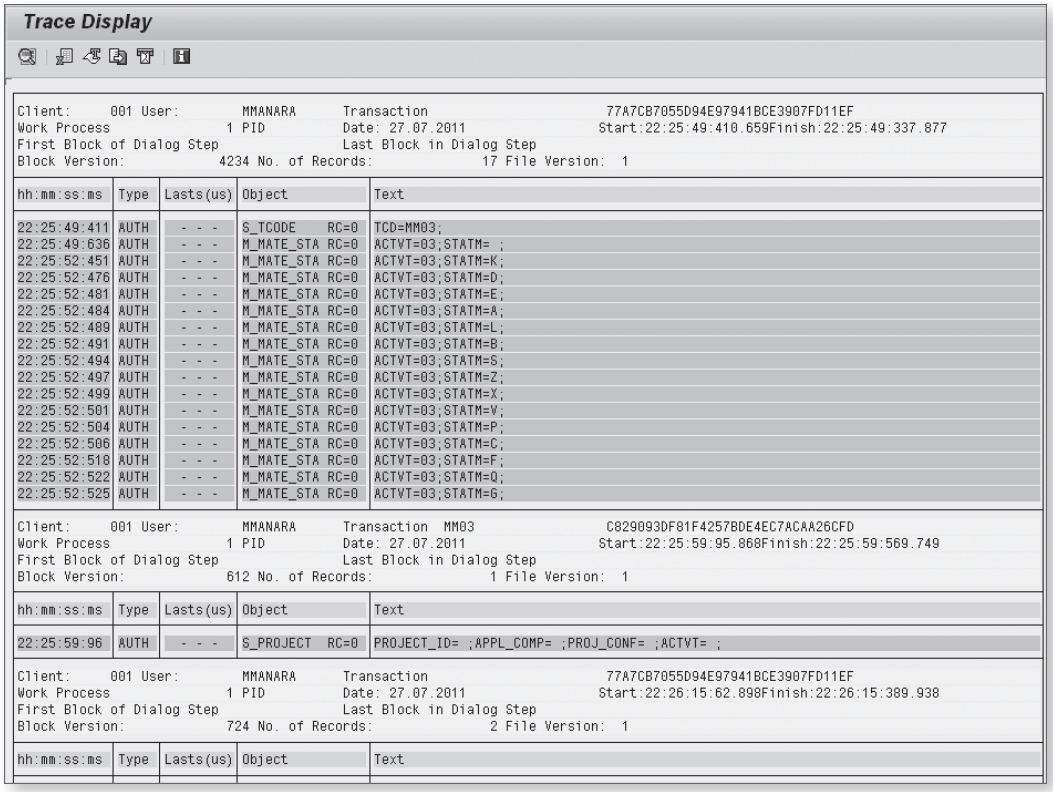


Figure 2 Selection Criteria in Trace Analysis

You'll now see the log that shows all authorization checks that have been performed in Figure 3. If the return code equals zero, the authorization check has passed. If the value is different from zero, the authorization check failed.



Trace Display

Client: 001 User: MMANARA Transaction 77A7CB7055D94E97941BCE3907FD11EF
Work Process 1 PID Date: 27.07.2011 Start:22:25:49:410.659Finish:22:25:49:337.877
First Block of Dialog Step Last Block in Dialog Step
Block Version: 4234 No. of Records: 17 File Version: 1

hh:mm:ss:ms	Type	Lasts(us)	Object	Text
22:25:49:411	AUTH	- - -	S_TCODE RC=0	TCD=MM03;
22:25:49:636	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM= ;
22:25:52:451	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=K;
22:25:52:476	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=D;
22:25:52:481	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=E;
22:25:52:484	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=A;
22:25:52:489	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=L;
22:25:52:491	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=B;
22:25:52:494	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=S;
22:25:52:497	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=Z;
22:25:52:499	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=X;
22:25:52:501	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=V;
22:25:52:504	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=P;
22:25:52:506	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=C;
22:25:52:518	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=F;
22:25:52:522	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=Q;
22:25:52:525	AUTH	- - -	M_MATE_STA RC=0	ACTVT=03;STATM=G;

Client: 001 User: MMANARA Transaction MM03 C829093DF81F4257BDE4EC7ACAA26CFD
Work Process 1 PID Date: 27.07.2011 Start:22:25:59:95.868Finish:22:25:59:569.749
First Block of Dialog Step Last Block in Dialog Step
Block Version: 612 No. of Records: 1 File Version: 1

hh:mm:ss:ms	Type	Lasts(us)	Object	Text
22:25:59:96	AUTH	- - -	S_PROJECT RC=0	PROJECT_ID= ;APPL_COMP= ;PROJ_CONF= ;ACTVT= ;

Client: 001 User: MMANARA Transaction 77A7CB7055D94E97941BCE3907FD11EF
Work Process 1 PID Date: 27.07.2011 Start:22:26:15:62.898Finish:22:26:15:389.938
First Block of Dialog Step Last Block in Dialog Step
Block Version: 724 No. of Records: 2 File Version: 1

hh:mm:ss:ms	Type	Lasts(us)	Object	Text

Figure 3 Authorization Trace Log

Let's quickly review a few important things to keep in mind when using Transaction ST01:

- Transaction ST01 is application server dependent. In other words, if your system has more than one application server (you can determine this by using Transaction SM51), you have to be sure that the Transaction ST01 trace is performed in the same application server the user is logged into. To do that, in Transaction SM51, you can perform a remote logon to another application server by typing Ctrl+Shift+F8 (see Figure 4).
- Take a look at your time zone and clock. If the application server has a time that is different from your PC, then during your analysis, after performing the trace, you might select a trace log outside the time recorded.

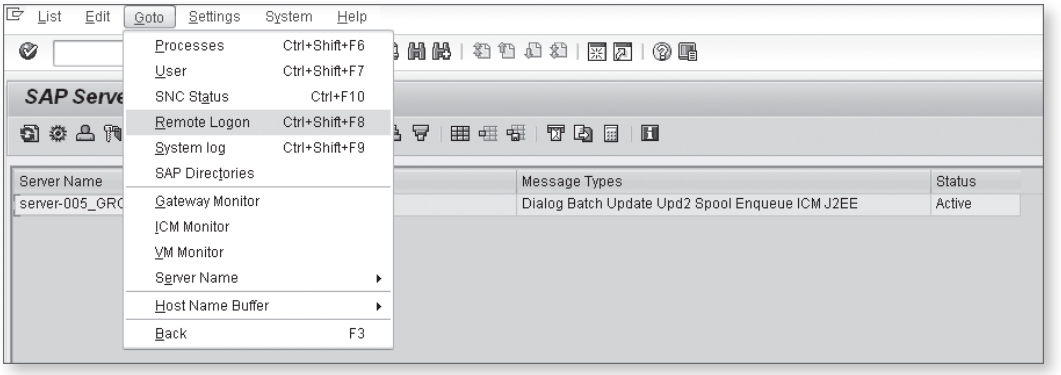


Figure 4 Perform a Remote Logon in Transaction SM51

- You can view in what application server a user is currently logged in to by using Transaction AL08 or by asking the user directly—he can see the application server name in the bottom-right area of your SAP GUI (Figure 5).

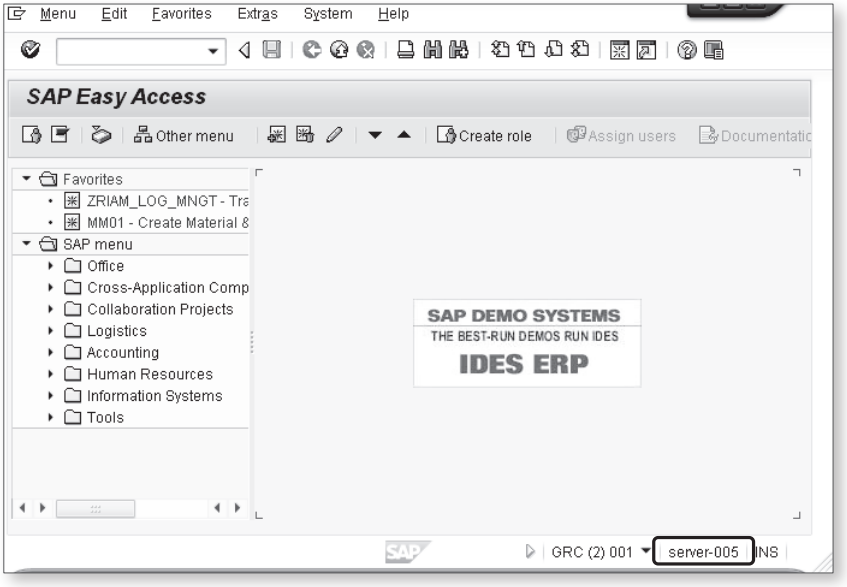


Figure 5 Discover the Application Server a User Is Logged In To

Tip 52

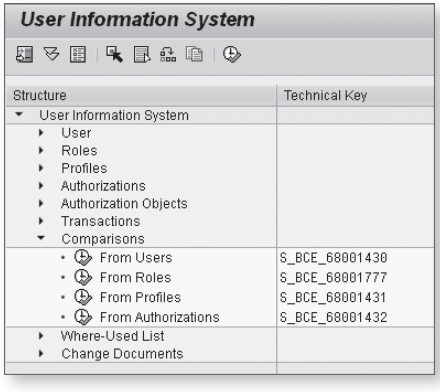
Comparing Authorization Roles to Check for Alignment Between Systems

You can easily compare two roles in different systems and check for alignment by using Transaction SUIM.

Comparing authorization roles is not a simple task if these roles contain several authorizations. Sometimes you may need to compare the same role if they have different values in the development system and quality system. This misalignment by the system is not in compliance using the transport management system. Through Transaction SUIM, you can easily compare two roles in a system or cross system.

And Here's How ...

Access Transaction SUIM to display the COMPARISONS tree shown in Figure 1.



« *Figure 1 Transaction SUIM Comparisons Tree*

Click on From Roles S_BCE_68001777. The screen shown in Figure 2 appears. Enter the role names you want to compare in the Role A and Role B fields.

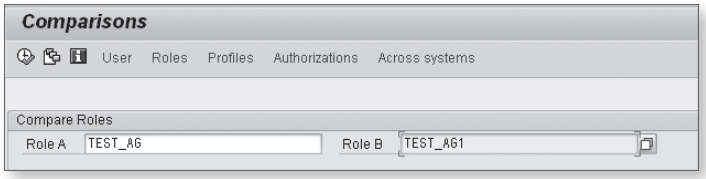


Figure 2 Role Comparison

Specify the system where you want the comparison performed by clicking on the Across systems button and then choosing the system ID name from the system list. For example, you can compare a role in the development system and a role in the production system. Note that to perform this functionality correctly, it's essential that the system's remote function call (RFC) destinations are defined.

The result of the comparison is shown in Figure 3. The Comparison column can display three different colors: Red means that different authorization objects exist between the roles, yellow indicates that the different roles have the same authorization objects but different values, and green indicates that the roles have the same authorization objects and same values. If the comparison is all green, that means the roles are equal. If you're seeing red or yellow, you can use Transaction PFCG to correct it.

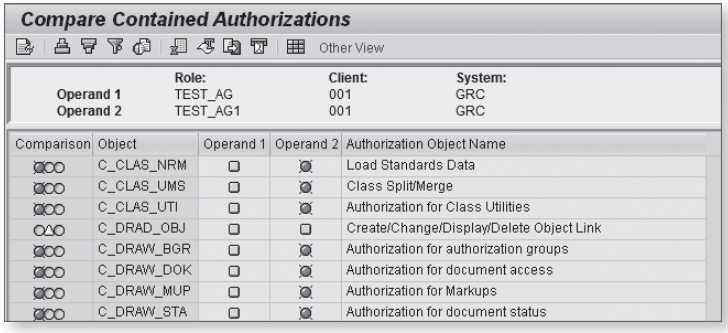


Figure 3 Comparison Result Example

Unfortunately, this transaction doesn't support a mass comparison between several roles at one time. However, you can go to *www.sdn.sap.com*, where you can find information on an enhancement that works around this limitation.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W