

NOTE JUNE 2007

The evaluation of the SysLog – SM21

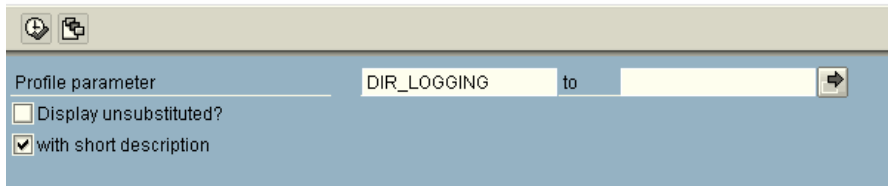
The SysLog is an acronym for “System Logging”. Selected events and problems within a SAP® system are generally logged.

The information are written into textfiles that are saved on the operation system level. The exact location can be identified with the help of the system parameter *DIR_LOGGING*.

Call the transaction **SA38**, and enter the report name **RSPFPAR**, push the key *F8*.

Enter the parameter name, and activate the execution via *F8*.

Display Profile Parameter



The name of the local file can be identified with the help of the parameter *rslg/local/file*.

The cross-client information are written sequentially into this file until the maximum file size is reached. The size is controlled via the parameter *rslg/max_diskspace/local*.

When the maximum limit is reached a new file will be created, and the old file will be saved as copy. This copy can be identified with the help of the parameter *rslg/local/old_file*.

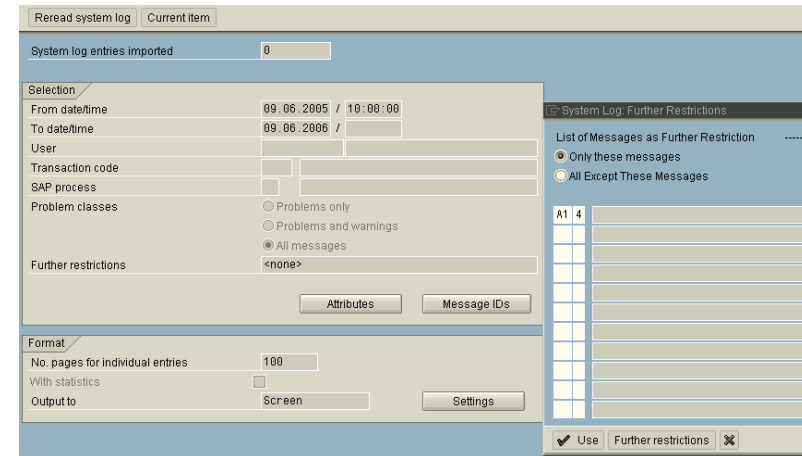
SAP® only saves one copy at a time. That means if the new file has reached the maximum size, it will be saved as a copy, and with this, the former copy will be overwritten.

A system log is written for every instance. If you run on multiple instances you have to make sure that you look up all corresponding log information. UNIX systems allow a central logging in that way, that the locally saved information can be send to a central instance [parameter *rslg/central/file*].

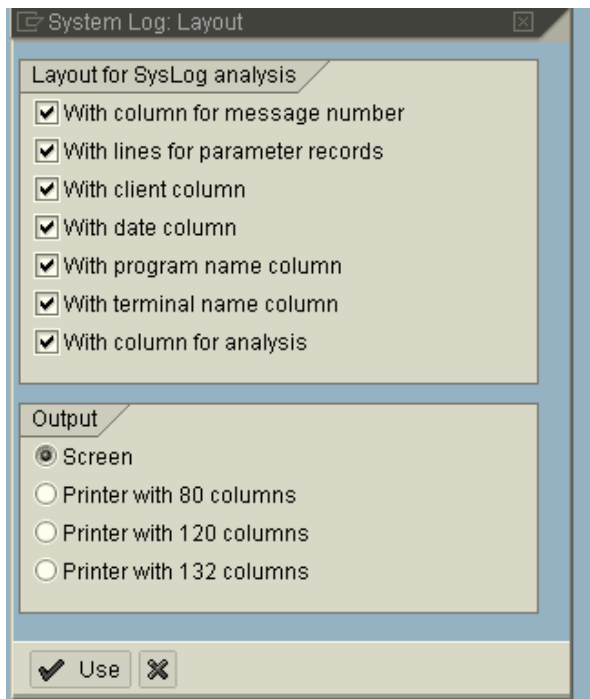
For evaluation of the records, please call the transaction **SM21** [the report RSLG0001 can be used as equivalent].

To check all remote instances at the same time [which is to be preferred due to efficiency] you have to select the menu path: *System log – Choose - All remote system logs*

Select then the menu path: *Edit – Expert mode*.



You can modify the layout via the menu path *Goto – Layout*.



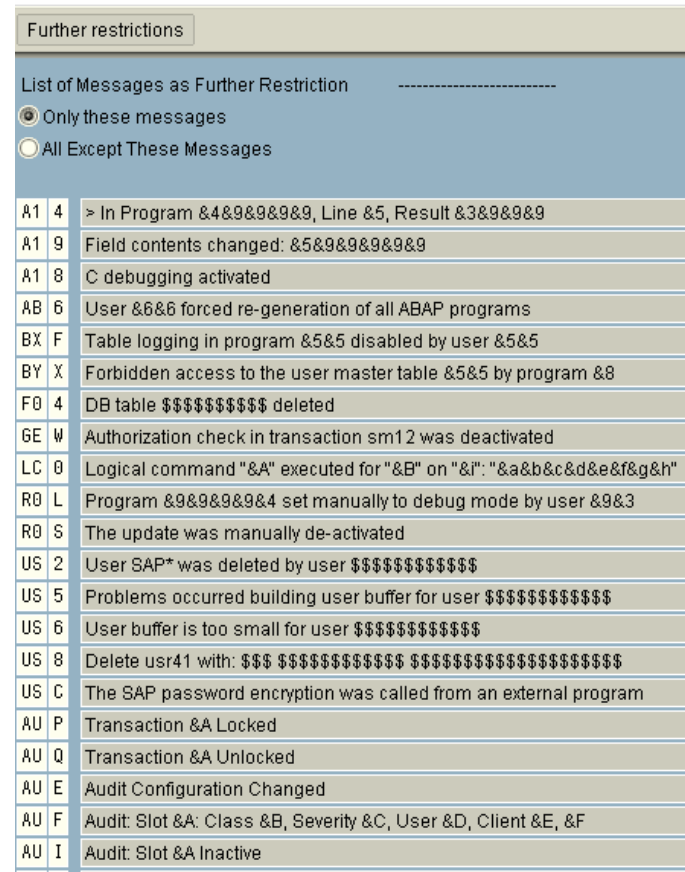
The required authorizations for the evaluation are

S_TCODE with TCD value SM21

S_ADMI_FCD with S_ADMI_FCD value SM21

The following events, and messages are important for audit and security reviews, and can be selected via the integrated button Message IDs.

System Log: Further Restrictions



You can get the full scope of possible entries by calling the table **TSL1D** via transaction **SE16N**.

A19 allows to review if a field content was changed in debug mode e.g., which is not allowed in a production environment. Together with the entries in *A14* you can even evaluate with which program, and which line.

With *BXF* you can see if the table logging was deactivated in a program by a user.

GEW shows if the authorization check for the lock management via **SM12** was deactivated.

LC0 displays if a user has executed logical os commands.

F04 provides the information about deletion of DB tables.

R0L allows you to see if a program was set to debug mode by a user.

R0S displays manually inactivation of the update, *R0T* the manual activation, and *R0U* shows if an update request was deleted. With *R0W* you can see if a terminated update was reposted. With *R0Y* you can show that terminated updates were displayed with **SM13**. And *R65* shows, that an update was terminated.

US2 shows if the user **SAP*** was deleted, and by whom.

AUP which transaction was locked, and with *AUQ* you can also see if, and which transaction was unlocked.

With *AUE* to *AUI* you can keep track of changes to the audit configurations of the Security Audit Log.

In the log, you can call the detail view via double click onto a selected entry.

Important note:

Please make sure that the access to the log files on the os level is restricted, and that the files are properly protected against unauthorized manipulations, or even deletion.