

EMC Security for SAP Enabled by RSA enVision
Technical Notes

August 2010

EMC Information Infrastructure Solutions

Copyright © 2010 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com

All other trademarks used herein are the property of their respective owners.

Part number: H7305

Table of Contents

Executive summary	5
Business case	5
Solution overview	5
Key results.....	5
Introduction.....	6
Contents	6
Purpose	6
Scope	6
Audience	6
Overview of RSA enVision.....	7
Introduction to RSA enVision	7
RSA enVision platform	7
RSA enVision <i>3-in-1</i> log management solution	8
Configuration of SAP system for integration of RSA enVision	10
Overview	10
Introduction.....	10
Components	10
Prerequisites	10
Contents	10
Environment.....	11
Product version information	11
Physical/virtual environment	11
RSA enVision solution for SAP lifecycle	12
SAP system configuration	13
Overview	13
1: Change the SAP configuration.....	13
2: Create the ZRSA database table	15
3: Create the ZRSAU_AS database table.....	19
4: Create the ZRSA message class	22
5: Create the ZRSAU_SELECT_EVENTS_JOB program	24
6: Create a variant for job scheduling	27
7: Schedule a background job.....	30
8: Configure the SAP security audit	32
SAP logs.....	34
Demos for customers	34
SAP system impact.....	35
Overview	35

Job run	35
SAP authorization.....	36
Job scheduling	36
Testing of SAP messages	37
Introduction to testing of SAP messages	37
SAP messages.....	37
Conclusion.....	39
Summary.....	39
Next steps	39

Executive summary

Business case Monitoring SAP logs for system changes, transports, user activity, and audit logs is challenging due to the number of locations an SAP administrator must visit per system to stay current with each system status. A central repository for logs eliminates any issues and enables users to perform Sarbanes-Oxley (SOX) and Governance Risk and Compliance (GRC) audits.

During problem resolution, users can start and stop SAP applications more than once. In some cases, SAP may only retain the previous version and current version of the log. Once the problem is solved, the original log disappears, making it difficult for an administrator to refer back to error messages in order to document how to keep the problem from reoccurring.

This RSA enVision® solution for SAP provides a central location for SAP logs by encompassing the database, storage, firewall, and network, along with numerous SAP messaging and audit logs. Logs can be retained for periods up to one year, enabling administrators to have historical data about changes to the SAP system, to determine if a problem has occurred in the past year, or to review logs over a business cycle in search of patterns of system behavior or other changes.

This Technical Note describes a solution that provides an integrated SAP/RSA enVision system, with a single location for accessing, managing, and analyzing logs and changes over the entire SAP landscape.

Solution overview In this solution, the SAP system is configured to include the integration of RSA enVision. By implementing RSA enVision as a SAP log management solution, customers have a single access point for all the system logs in their landscape. RSA enVision provides, on demand, a complete history of the logs and changes for all the layers in the SAP landscape.

To ensure the reliability of the auditing and reports, EMC completed testing of 37 different SAP messages and different audit logs in both physical and virtual environments. For more information, see the 'Testing of Messages' section.

Key results Once the SAP system has been configured and RSA enVision is fully integrated, customers can perform all the tasks associated with log management of the SAP landscape.

Testing of SAP messages confirms that the auditing and reports functions of the solution are reliable.

Introduction

Contents

This Technical Note includes the following sections:

Topic	See Page
Overview of RSA enVision	7
Configuration of SAP system for integration of RSA enVision	10
Testing of SAP messages	37
Conclusion	39
References	40

Purpose

This Technical Note provides the required steps to integrate the RSA enVision log management solution with an SAP system and briefly documents the testing of SAP messages.

Scope

The scope of this Technical Note is to:

- Describe the process for changing the SAP configuration
- Describe the process for creating SAP database tables and message classes
- Describe the processes for creating a job, a variant for job scheduling, and a background job
- Describe the process for configuring the SAP security audit
- Document the impact, if any, to the SAP system once configuration is complete
- Document the messages that were tested and provide a brief description of each one

This will allow RSA enVision to receive the SAP data.

Note The installation and configuration of RSA enVision is not within the scope of this Technical Note and is a prerequisite to using this solution.

Audience

This Technical Note is intended for customers, partners, and EMC employees, including IT planners, SAP and storage architects, basis administrators, and any others involved in evaluating, acquiring, managing, operating, or designing an SAP landscape infrastructure.

It is assumed that the audience is familiar with the SAP system and RSA enVision.

Overview of RSA enVision

Introduction to RSA enVision

The RSA enVision platform is the market-leading solution for Security Information and Event Management (SIEM). It gives organizations a single, integrated 3-in-1 log management solution for simplifying compliance, enhancing security and risk mitigation, and optimizing IT and network operations through the automated collection, analysis, alerting, auditing, reporting, and security storage of all logs.

In any IP network, almost every device – from firewalls to servers – generates logs of the traffic it carries, the transactions it makes, and the activities it conducts. This data is vital to secure successful use of the network. It helps to optimize security, business continuity, and network performance, and provides an essential record of all network events and user activity, helping comply with government, industry, and internal regulations.

But monitoring thousands of devices and then handling and protecting the event log data each device produces – covering many thousands of events, every second of every day – can be a huge challenge. The RSA enVision platform addresses this challenge and makes it easy for your compliance, security, and network professionals to identify, explore, and resolve critical events and trends by building a clear and comprehensive picture of network activity.

RSA enVision platform

The RSA enVision platform can capture, manage, and analyze events from the entire network infrastructure out-of-the-box, without requiring agents, using event transport protocols, such as secure file transfer. Data is stored unchanged, intact, and tamperproof. In addition, you can access and retrieve it for any compliance purpose, now or in the future.

Figure 1 shows the platform architecture of RSA enVision and its lifecycle for collecting, managing, and analyzing information.

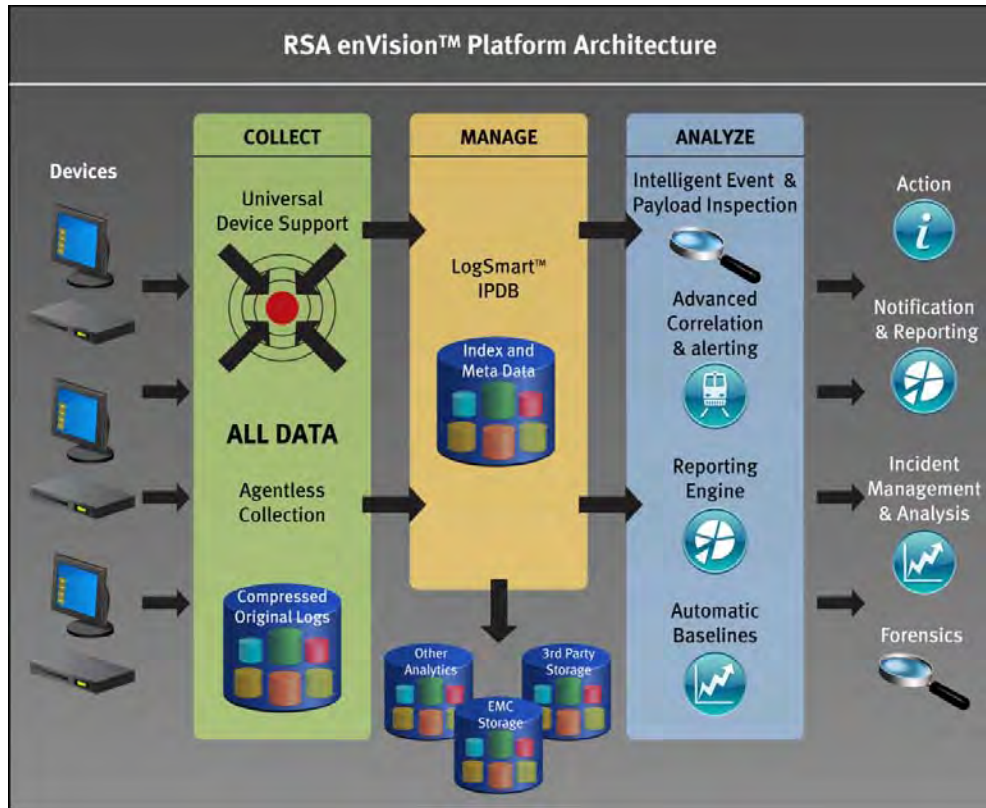


Figure 1. RSA enVision platform architecture

RSA enVision 3-in-1 log management solution

The main benefits of using the RSA enVision 3-in-1 log management solution are:

Simplified Compliance

Administrators can automatically collect log data about network, file, application, and user activity that can significantly help simplify the compliance process. Included are over 1,100 reports that are tailored to today's specific compliance requirements.

The solution also simplifies compliance with whatever legislation emerges in years to come, because it stores all log data without filtration or normalization and protects it from tampering, providing a verifiably authentic source of archived data.

Enhanced Security and Risk Mitigation

With real-time security event alerts, monitoring, and drill-down forensic functionality, the platform gives administrators a clear view of important information. Because they can see and understand the threats and risks, they can take more effective actions to mitigate those risks.

Optimized IT and Network Operations

Managed log data is the best source of information about infrastructure performance and user behavior. IT support staff can use the RSA enVision platform to track and manage activity logs for servers, networking equipment, and storage platforms, as well as monitor network assets, the availability and status of people, and hardware and business applications.

EnVision provides an intelligent forensic tool for troubleshooting infrastructure problems and protecting infrastructure resources, assisting IT managers in help desk operations, and providing granular visibility into specific behaviors by end users.

See Figure 2 for details.

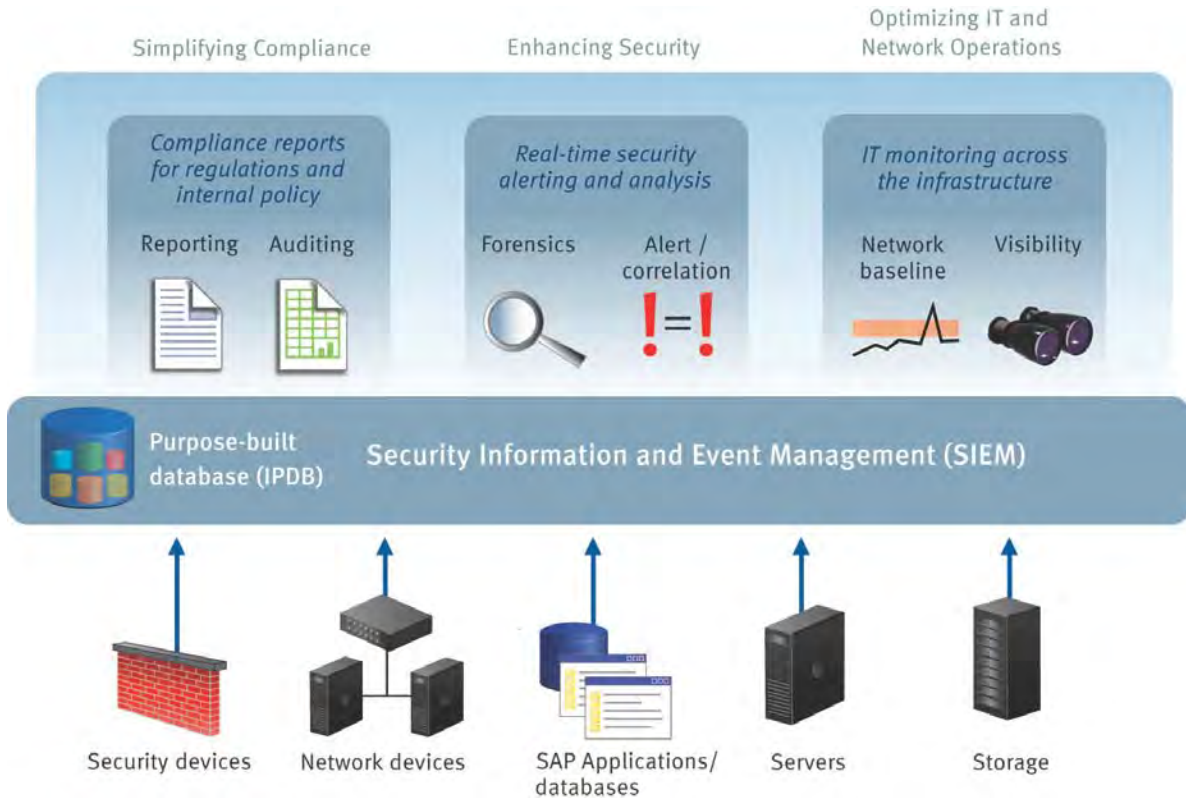


Figure 2. RSA eVision log management platform

Configuration of SAP system for integration of RSA enVision

Overview

Introduction

Once customers install RSA enVision, they need to configure the SAP system so that they can integrate enVision with the SAP landscape.

The SAP system is configured so that:

- Customers can capture all security events SAP system activity
- Customers can capture any user role activities
- Customers can capture any job activity

This solution was tested on the following configuration:

- An SAP landscape with a virtualized system including at least two SAP machines

For detailed information about SAP system installation, refer to the relevant SAP installation guides.

Components

The solution uses the following components and technologies:

- RSA enVision
 - SAP ECC 6.0
 - XML messaging
 - Secure file transfer protocol (FTP)
-

Prerequisites

Before customers can configure the SAP system, they must do the following:

- Install RSA enVision software
For more detailed information, refer to the *RSA enVision Install Guide*.
 - Procure the ZRSAU_SELECT_EVENTS_JOB script from RSA
-

Contents

This section contains the following topics:

Topic	See Page
Environment	11
SAP system configuration	13
SAP system impact	35

Environment

Product version information

Table 1 and Table 2 show product version information for the SAP ECC Enterprise event source and RSA enVision.

Table 1. Event source (device)

Details	Product information
New or Updated	New - RSA has developed new event source XML definition sets for the SAP ECC Enterprise event source
Vendor	SAP
Event Source (Device)	ECC
Supported Versions/Platforms	4.6C Service Pack 2 to NW7.2

Table 2. RSA enVision

Details	Product information
Version	3.5.1 and higher
Event Source (Device) Type	SAP, 121
Collection Method	File Reader (SFTP)
Event Source (Device) Class.Subclass	Host.Application Server
Service	NIC File Reader

Physical/virtual environment

Users can apply the solution to an SAP landscape that is composed of either:

- A physical system
- A virtualized system

SAP ABAP code works regardless of whether the system is physical or virtual.

RSA enVision solution for SAP lifecycle

Figure 3 outlines the lifecycle of the integrated RSA enVision solution with the SAP landscape.

A user logs in to the SAP landscape and runs a job to generate an audit or report on the changes and logs for a selected time period. The enVision program collects the log information from the various SAP and non-SAP systems within all levels of the landscape. The requested audit or report is generated.

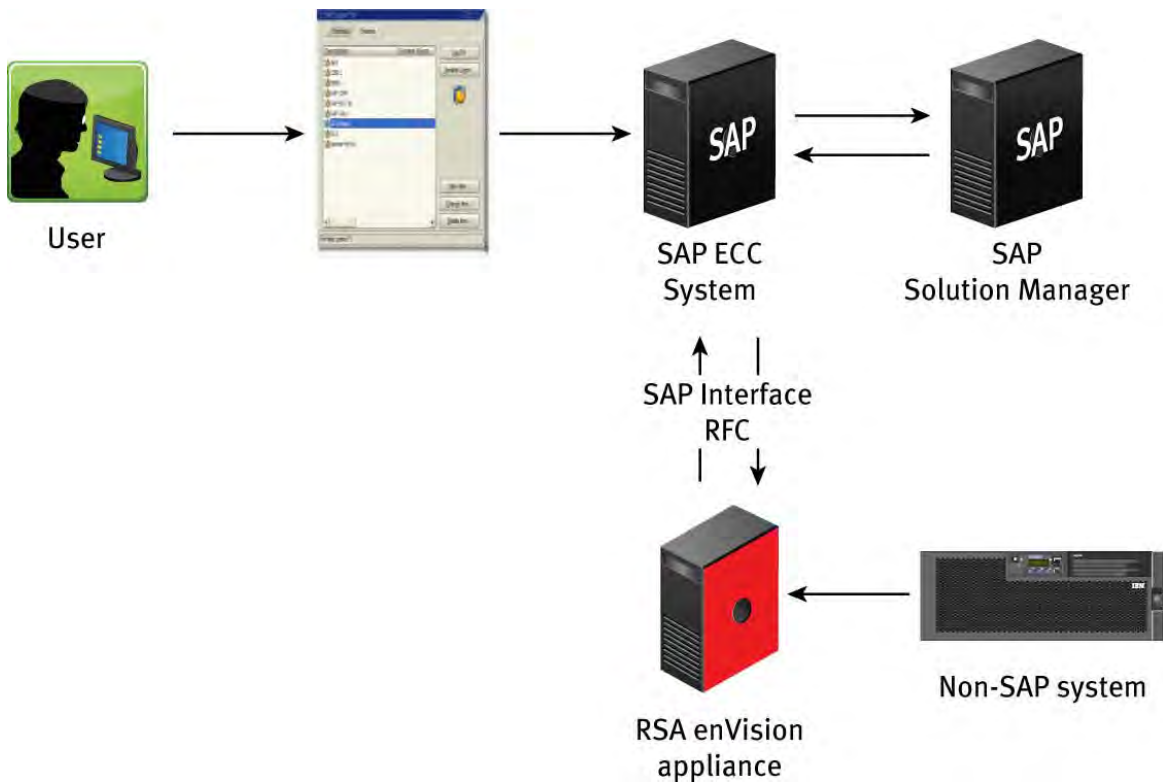


Figure 3. RSA enVision solution for SAP

SAP system configuration

Overview


This section contains information on configuring the SAP system as follows:

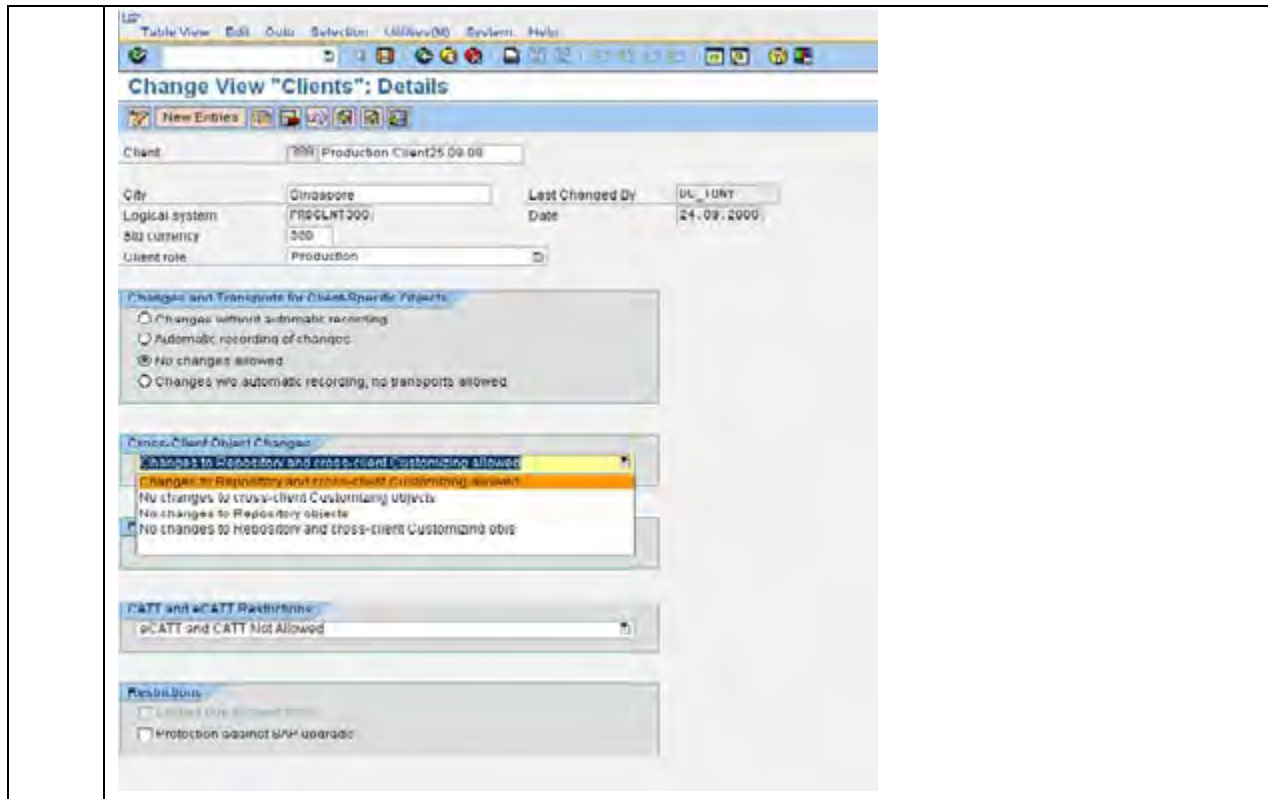
1. Change the SAP configuration
2. Create ZRSA database table
3. Create ZRSAU_AS database table
4. Create ZRSA message class
5. Create ZRSAU_SELECT_EVENTS_JOB program
6. Create a variant for job scheduling
7. Schedule a background job
8. Configure the SAP security audit

For detailed information on each procedure, see the steps below.

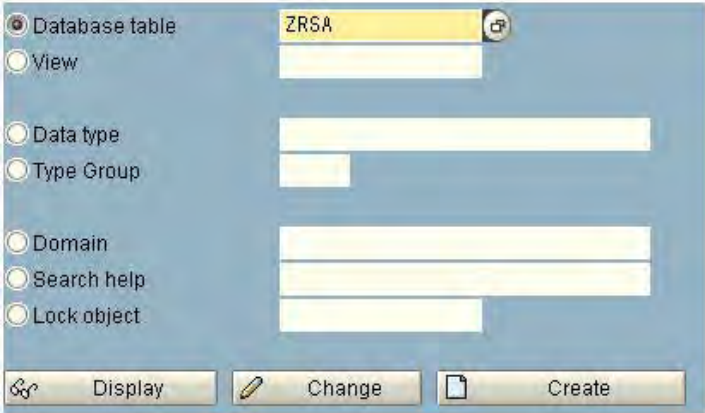

1: Change the SAP configuration

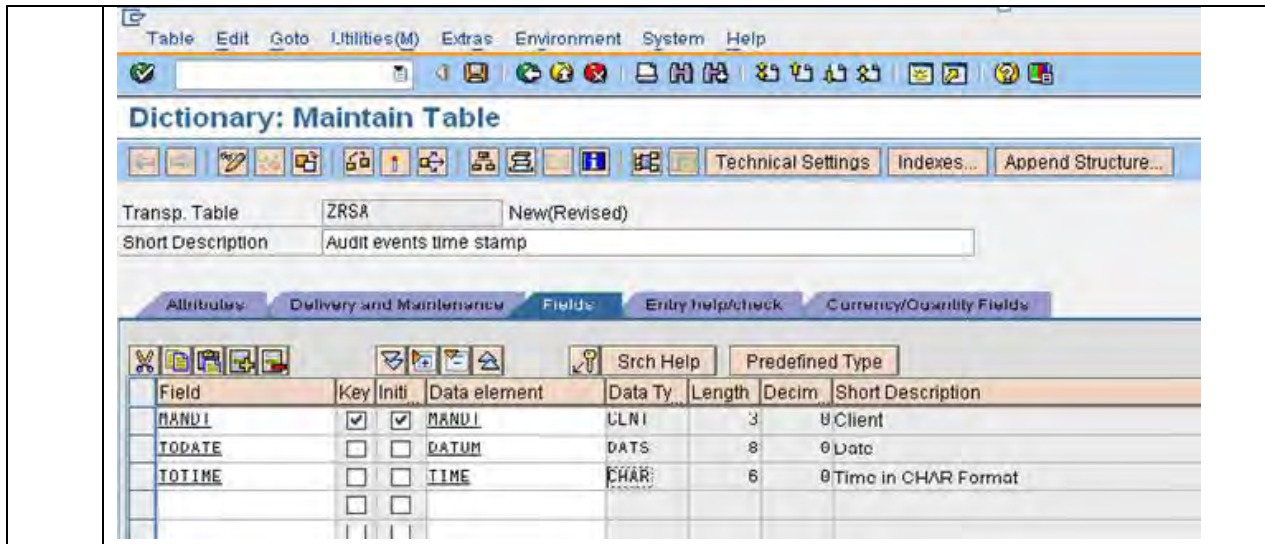
The following table shows the steps for changing the SAP configuration.

Step	Action
1	To access the ABAP Editor, log in to SAP using the appropriate user account. 
2	In the Command field, type <code>SCC4</code> and press ENTER.
3	In the Change View “Clients”: Details window, under Cross-Client Object Changes , choose Changes to Repository and cross-client Customizing allowed .



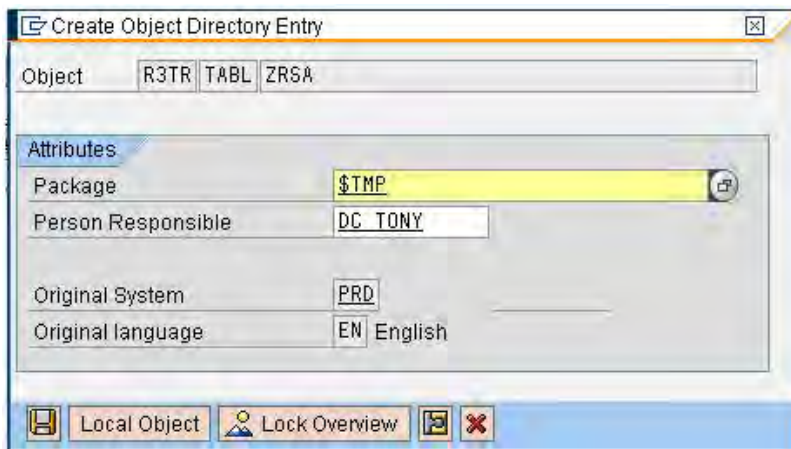
2: Create the ZRSA database table The following table shows the steps for creating the ZRSA database table.

Step	Action
1	To create a database table, in the Command field, type <i>SE11</i> and press ENTER.
2	In the Database table field, type <i>ZRSA</i> , then click Create . 
3	In Short Description , type a short description of the table.
4	Select the Delivery and Maintenance tab. In Delivery Class , enter <i>A</i> for Application Table.
5	In the Data Browser/Table View Maint. , select Display/Maintenance Allowed with Restrictions . 
6	Select the Fields tab, then enter the following table fields and data elements: <ul style="list-style-type: none"> • Field: MANDI, Data element: MANDI • Field: TODATE, Data element: DATUM • Field: TOTIME, Data element: TIME

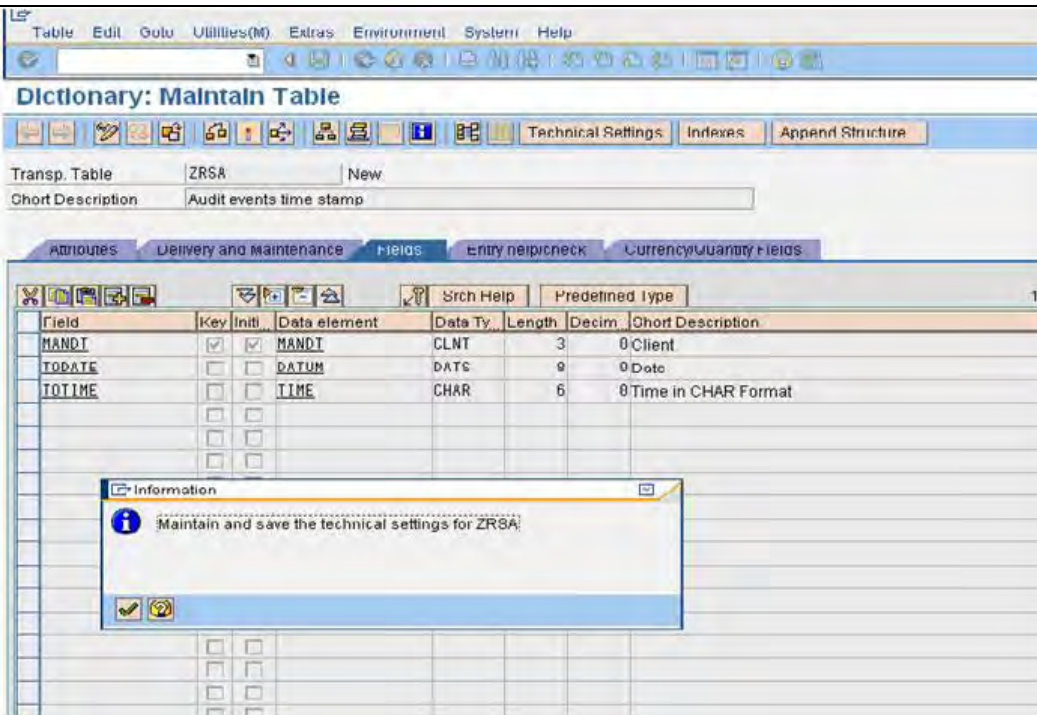


7 To save all the changes made, click **Save**.

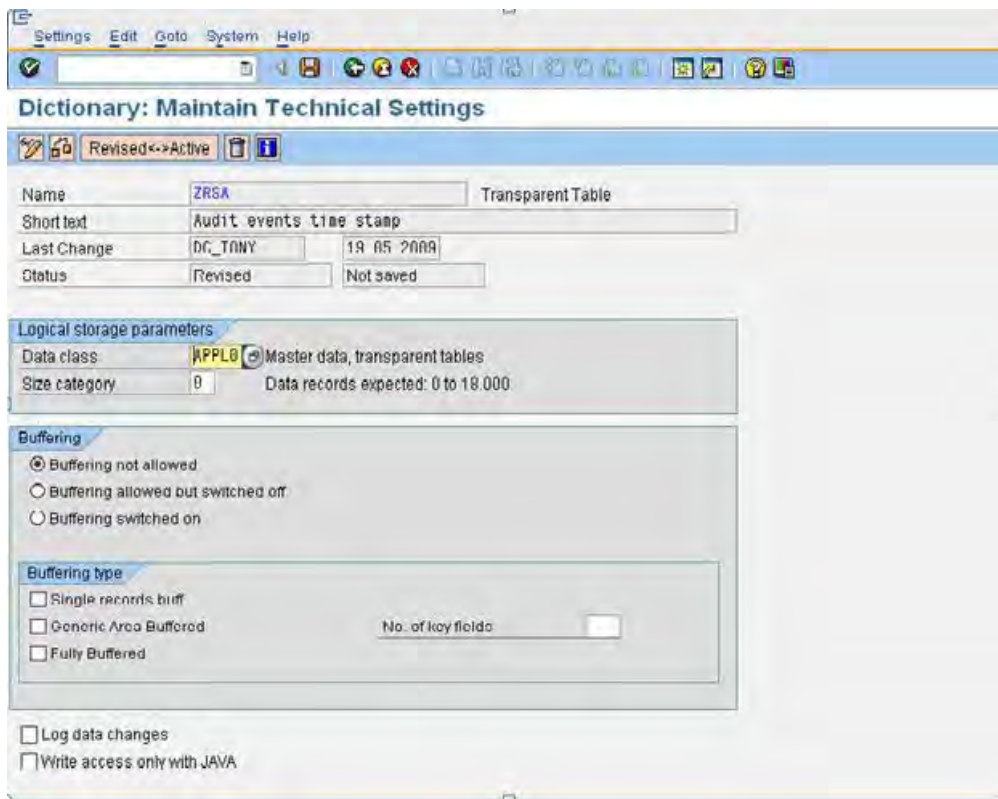
8 When the **Create Object Directory Entry** dialog box appears in the window, in **Package**, type **\$TMP**, then click **Save**.



9 To maintain and save the technical settings for ZRSA, click the **Activate** icon in the toolbar. To close the information window, click the checkmark icon.



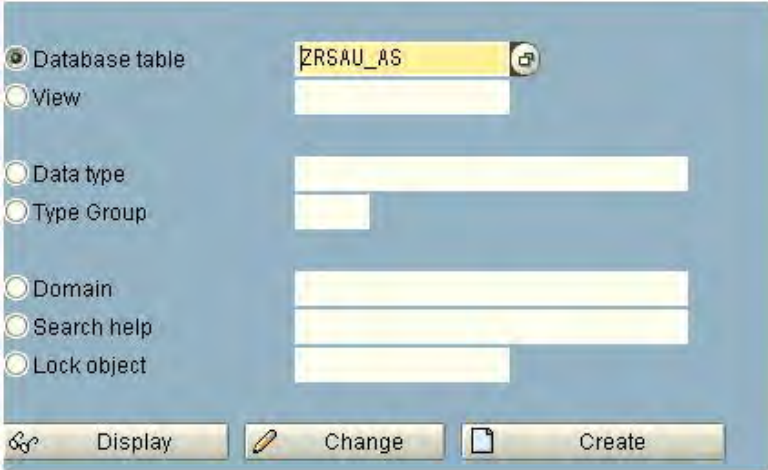
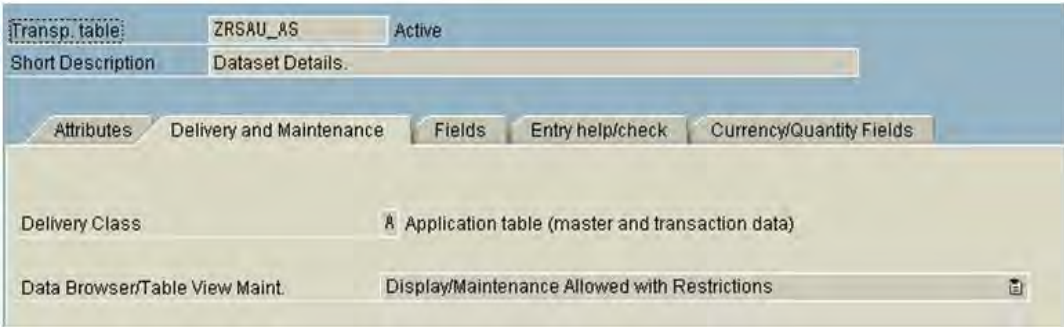
- 10 To edit the technical settings, click **Technical Settings**.
- In **Data class**, type *APPL0* and in **Size category**, type *0*.
 - Under **Buffering**, choose **Buffering not allowed**.
 - Click **Save**.

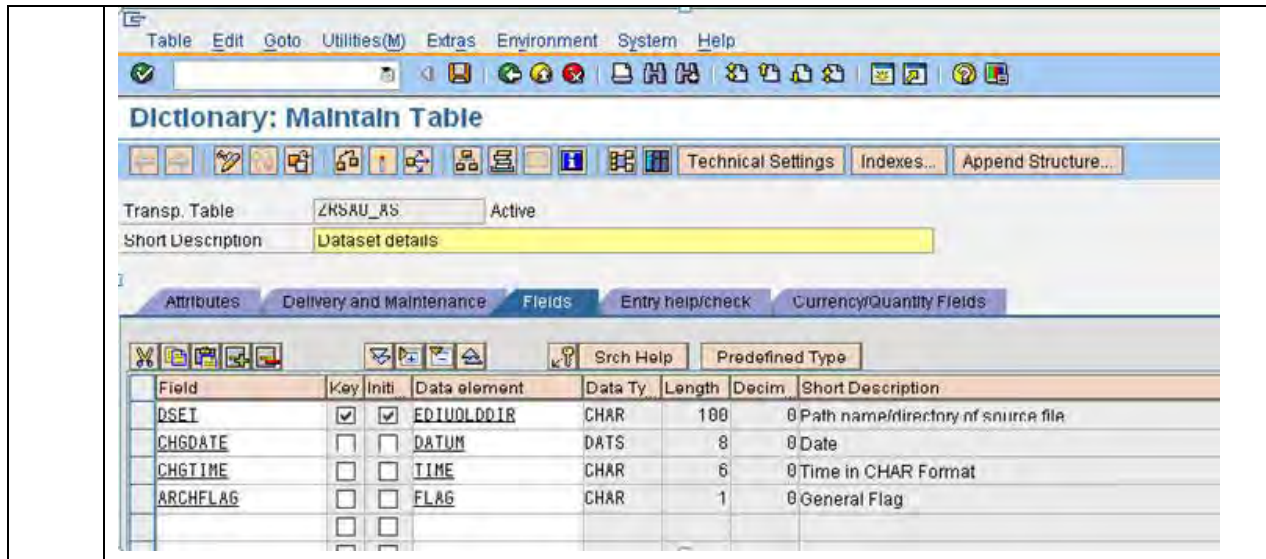


11	Click the Activate icon in the toolbar. The ZRSA database table is created.
----	---------------------------------------------------------------------------------------

3: Create the ZRSAU_AS database table

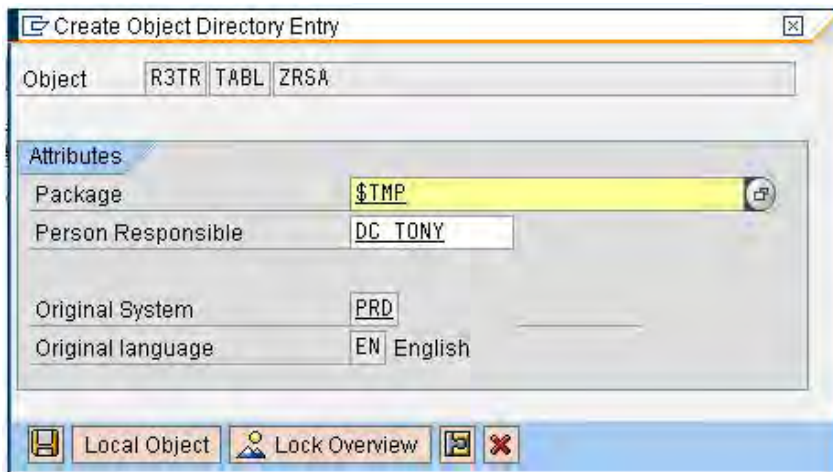
The following table shows the steps for creating the ZRSAU_AS database table.

Step	Action
1	To create a database table, in the Command field, type <i>SE11</i> and press ENTER.
2	In the Database table field, type <i>ZRSAU_AS</i> , then click Create . 
3	In Short Description , type a short description of the table.
4	Select the Delivery and Maintenance tab. In Delivery Class , enter <i>A</i> for Application table .
5	In the Data Browser/Table View Maintenance , select Display/Maintenance Allowed with Restrictions . 
6	Select the Fields tab, then enter the following table fields and data elements: <ul style="list-style-type: none"> • Field: DSET; Data element: EDIUOLDDIR • Field: CHGDATE; Data element: DATUM • Field: CHGTIME; Data element: TIME • Field: ARCHFLAG; Data element: FLAG



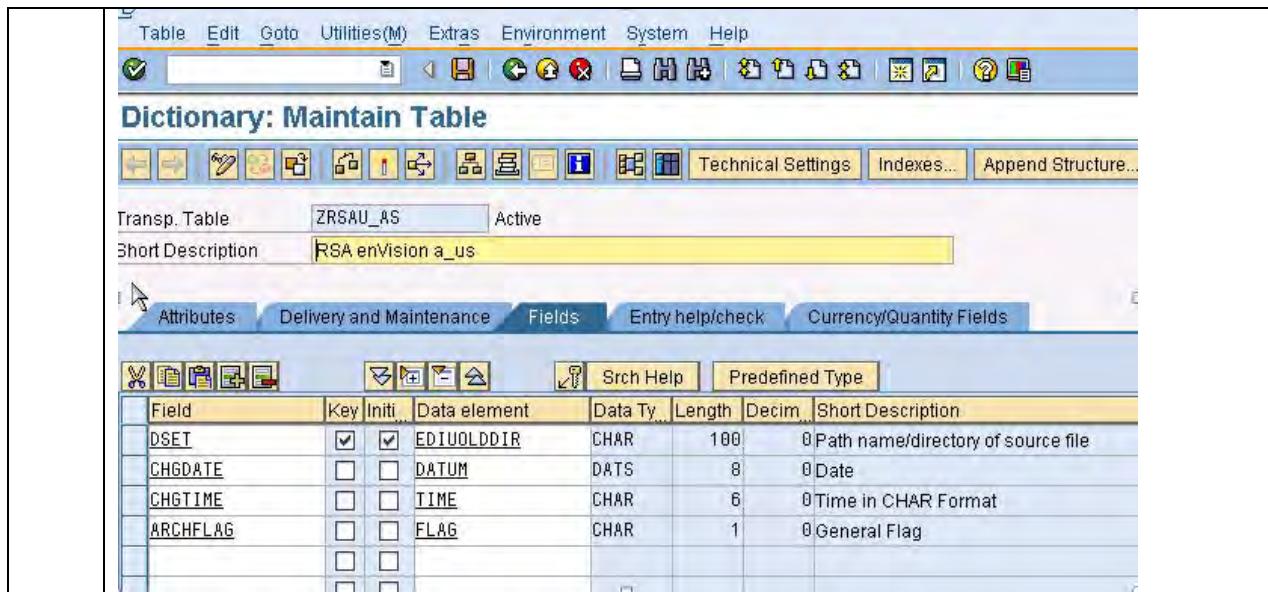
7 To save all the changes made, click **Save**.

8 When the **Create Object Directory Entry** dialog box appears in the window, in **Package**, type **\$TMP**, then click **Save**.

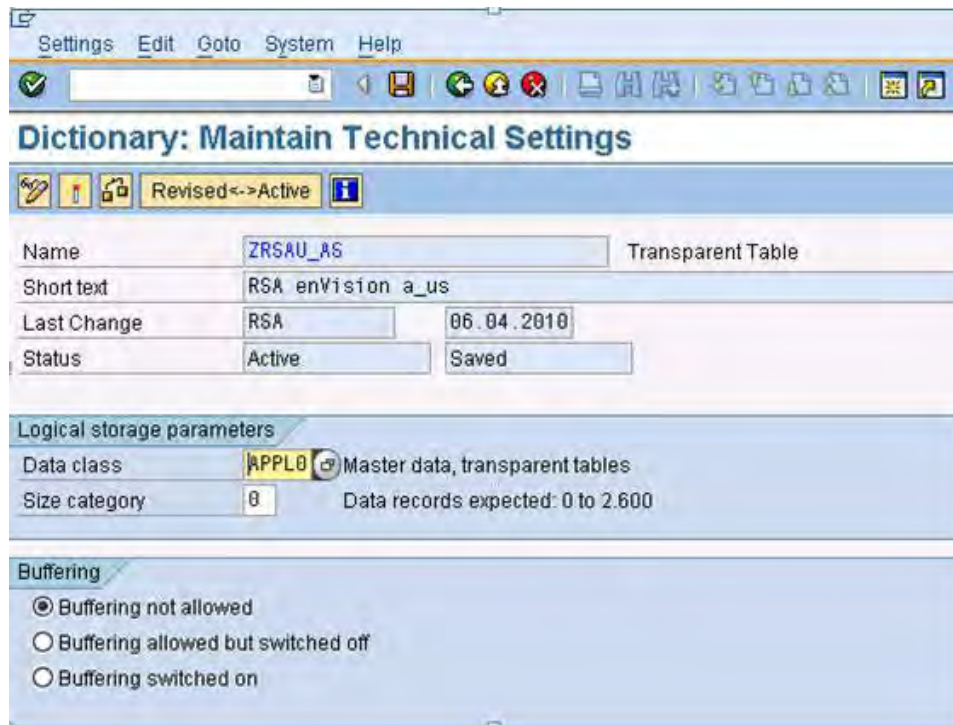


9 To maintain and save the technical settings for ZRSAU_AS, click the **Activate** icon in the toolbar.

To close the information window, click the checkmark icon.

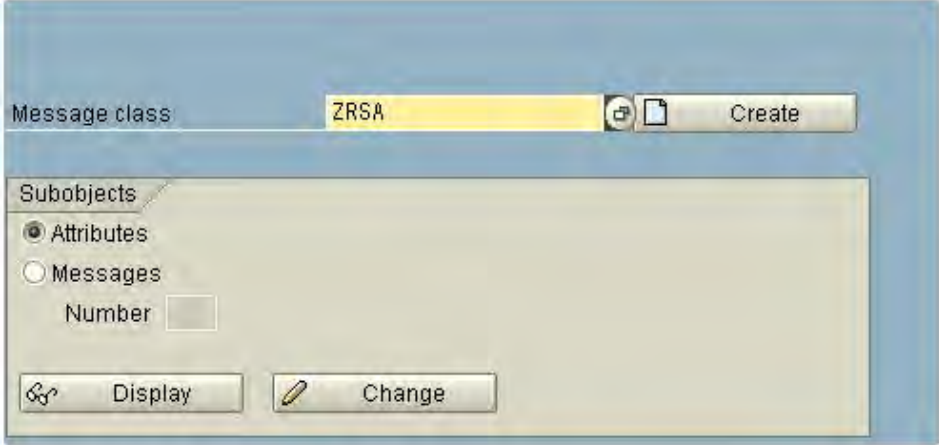
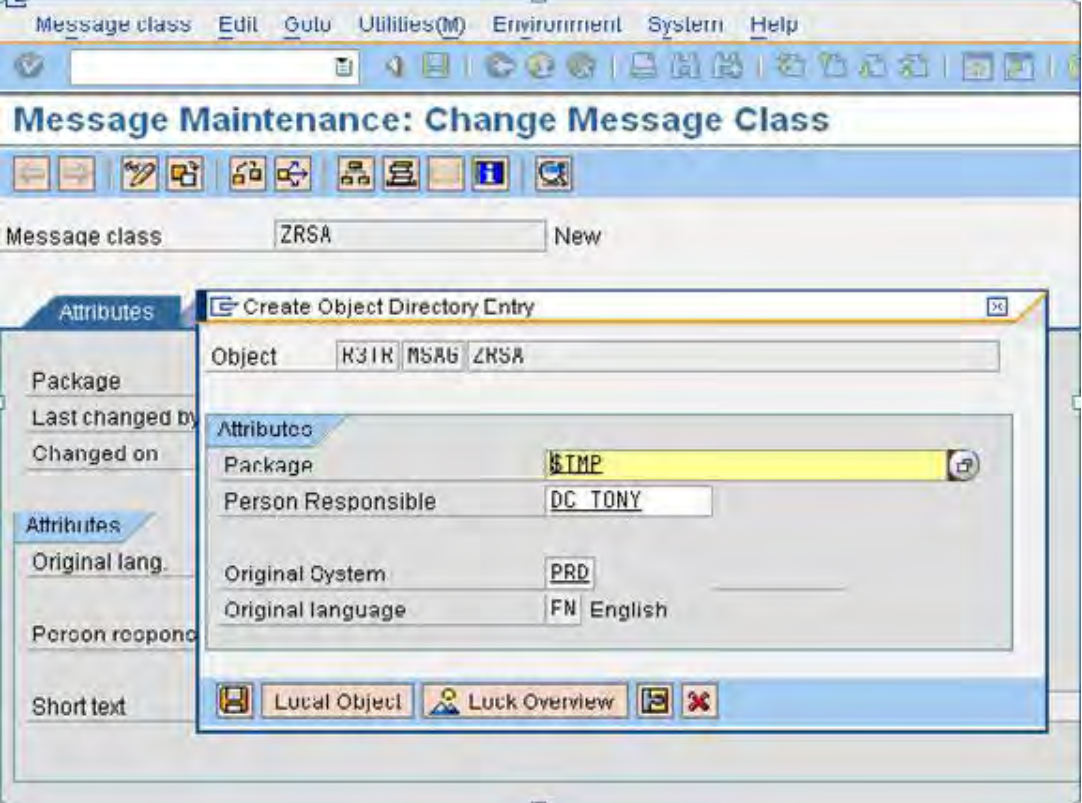


- 10 To edit the technical settings, click **Technical Settings**, then:
- In **Data class**, type *APPL0* and in **Size category**, type *0*.
 - Under **Buffering**, choose **Buffering not allowed**.
 - Click **Save**.



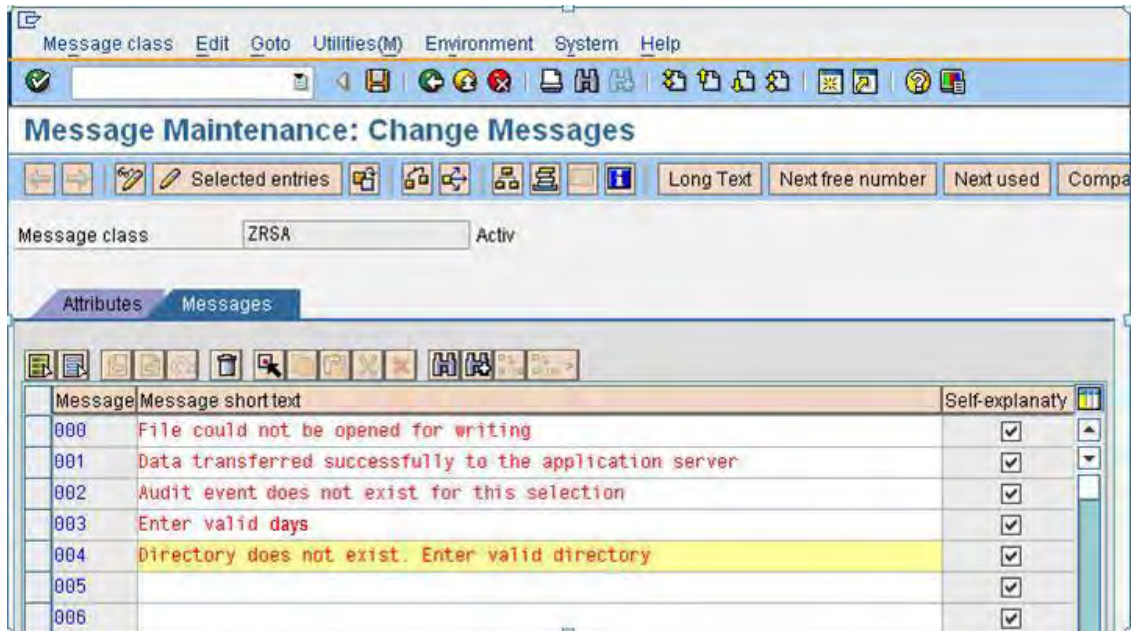
- 11 Click the **Activate** icon in the toolbar.
The ZRSAU_AS database table is created.

4: Create the ZRSA message class The following table shows the steps for creating the ZRSA message class to display messages in the ZRSAU_SELECT_EVENTS_JOB program.

Step	Action
1	In the Command field, type <i>SE91</i> and press ENTER.
2	In Message class type <i>ZRSA</i> , then click Create . 
3	When the Create Object Directory Entry dialog box appears in the window, in Package , type <i>\$TMP</i> , then click Save . 

4 Select the **Messages** tab, then type the following message short texts next to the following message numbers:

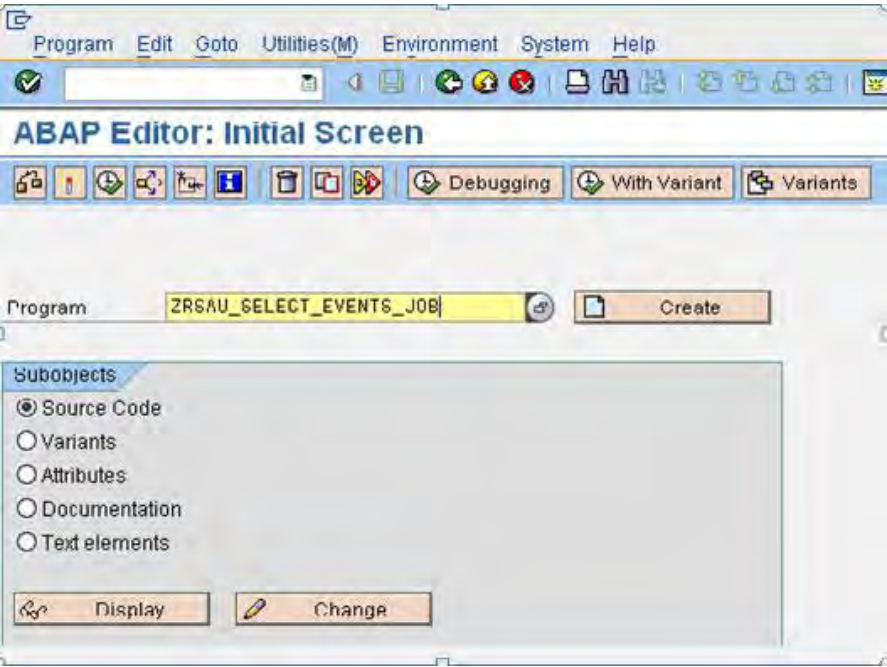
- 000: File could not be opened for writing.
- 001: Data transferred successfully to the application server.
- 002: Audit event does not exist for this selection.
- 003: Enter valid days.
- 004: Directory does not exist. Enter valid directory.



5 Click **Save**.
Message class ZRSA is created.

5: Create the ZRSAU_SELECT_EVENTS_JOB program

The following table shows the steps for creating the ZRSAU_SELECT_EVENTS_JOB program.

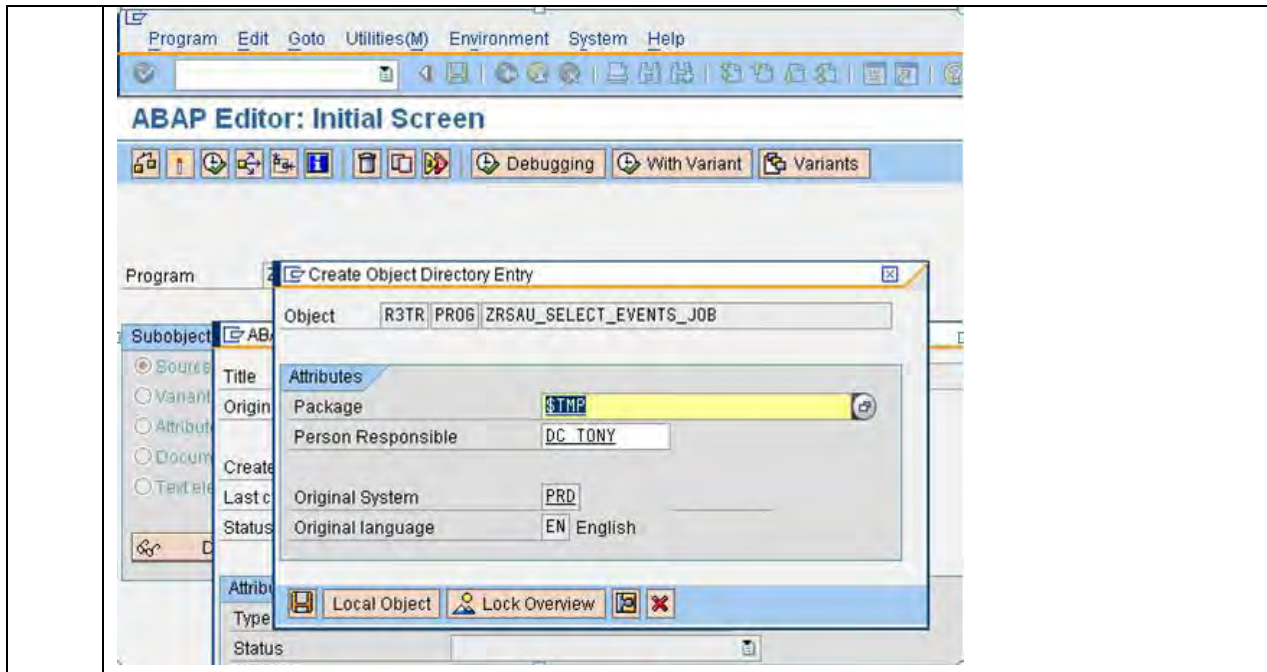
Step	Action
1	In the Command field, type <i>SE38</i> and press ENTER.
2	<p>In Program, type <i>ZRSAU_SELECT_EVENTS_JOB</i> and click Create.</p>  <p>The screenshot shows the 'ABAP Editor: Initial Screen' window. At the top, there is a menu bar with 'Program', 'Edit', 'Goto', 'Utilities(M)', 'Environment', 'System', and 'Help'. Below the menu bar is a toolbar with various icons. The main area of the window has a 'Program' field containing the text 'ZRSAU_SELECT_EVENTS_JOB' and a 'Create' button to its right. Below this is a 'Subobjects' section with a list of options: 'Source Code' (selected with a radio button), 'Variants', 'Attributes', 'Documentation', and 'Text elements'. At the bottom of the 'Subobjects' section are 'Display' and 'Change' buttons.</p>
3	<p>a) In the Program Attributes dialog box, in Title, type <i>RSA_ZRSAU_JOB</i>. b) In the Attributes section, in Type, choose Executable program. c) Click Save.</p>

The screenshot shows the ABAP Editor interface. At the top, there is a menu bar with 'Program', 'Edit', 'Goto', 'Utilities(M)', 'Environment', 'System', and 'Help'. Below the menu bar is a toolbar with various icons. The main window title is 'ABAP Editor: Initial Screen'. In the center, there is a 'Program' field containing 'ZRSAU_SELECT_EVENTS_JOB' and a 'Create' button. Below this, a dialog box titled 'ABAP: Program Attributes ZRSAU_SELECT_EVENTS_JOB Change' is open. The dialog box has a left sidebar with radio buttons for 'Source', 'Variant', 'Attribut', 'Docum', and 'Text ele'. The main area of the dialog box contains the following fields and options:

- Title: RSA_ZRSAU_JOB
- Original language: EN English
- Created: 19.05.2009 DC_TONY
- Last changed by: [empty]
- Status: New(Revised)
- Attributes section:
 - Type: Executable program
 - Status: [empty]
 - Application: [empty]
 - Authorization Group: [empty]
 - Logical database: [empty]
 - Selection screen: [empty]
 - Editor lock
 - Fixed point arithmetic
 - Unicode checks active
 - Start using variant

At the bottom of the dialog box, there is a 'Save' button and other standard window control icons.

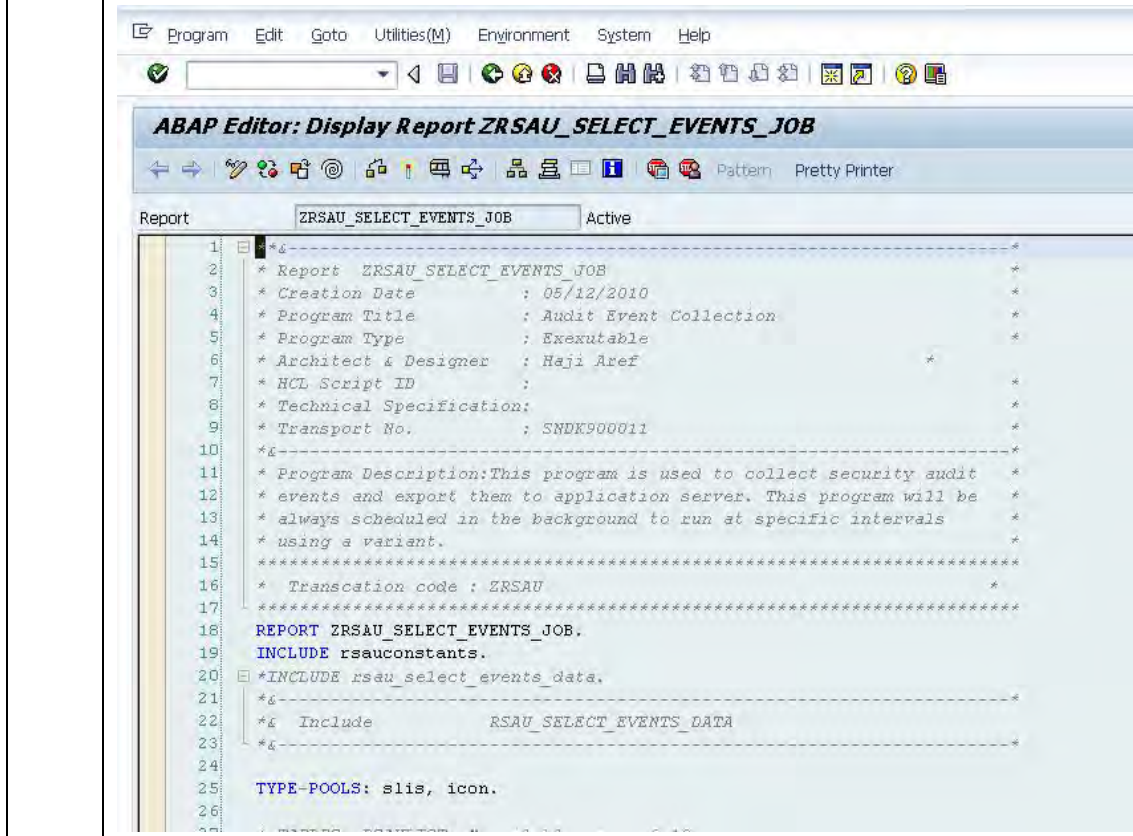
4 When the **Create Object Directory Entry** dialog box appears in the window, in **Package**, type **\$TMP**, then click **Save**.



5 Copy the contents of the ZRSAU_SELECT_EVENTS_JOB script provided by RSA to the ABAP Editor.

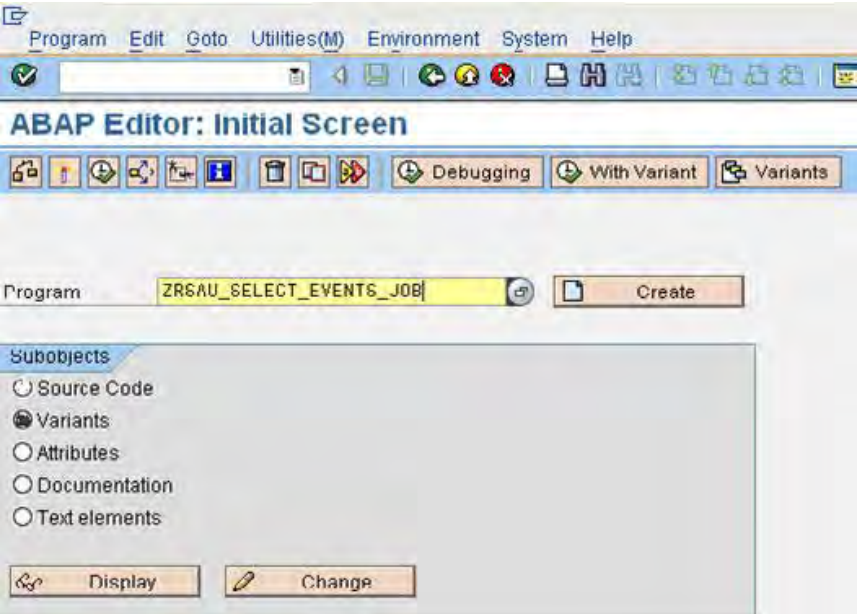
6 Click **Save**, then click **Check** to check for any errors.

7 To see the **Change Report**, click **Activate**.



6: Create a variant for job scheduling

The following table shows the steps for creating a variant for job scheduling.

Step	Action
1	In the Command field, type <i>SE38</i> and press ENTER.
2	<p>In the Initial Screen, under Subobjects, choose Variants, then click Create. In Program, type <i>ZRSAU_VARIANT</i>.</p> 
3	Click Create .
4	<p>Enter the appropriate information in the following fields:</p> <ul style="list-style-type: none"> • From Date/Time • To Date/Time • Name of the Directory • Name of the Audit File • Days to keep

5	<p>Under Audit Classes, select all classes and events checkboxes. Under Events, choose Every.</p>
6	<p>Click Attributes.</p>
7	<p>a) In the Variant Attributes window, in Meaning, type <i>variant</i>. b) Select the Only for Background Processing checkbox. c) Click Save.</p>

Variant Edit Goto Environment System Help

Variant Attributes

Copy Screen Assignment

Variant Name: ZRSAU_VARIANT
 Meaning: variant

Only for Background Processing
 Protect Variant
 Only Display in Catalog
 System Variant (Automatic Transport)

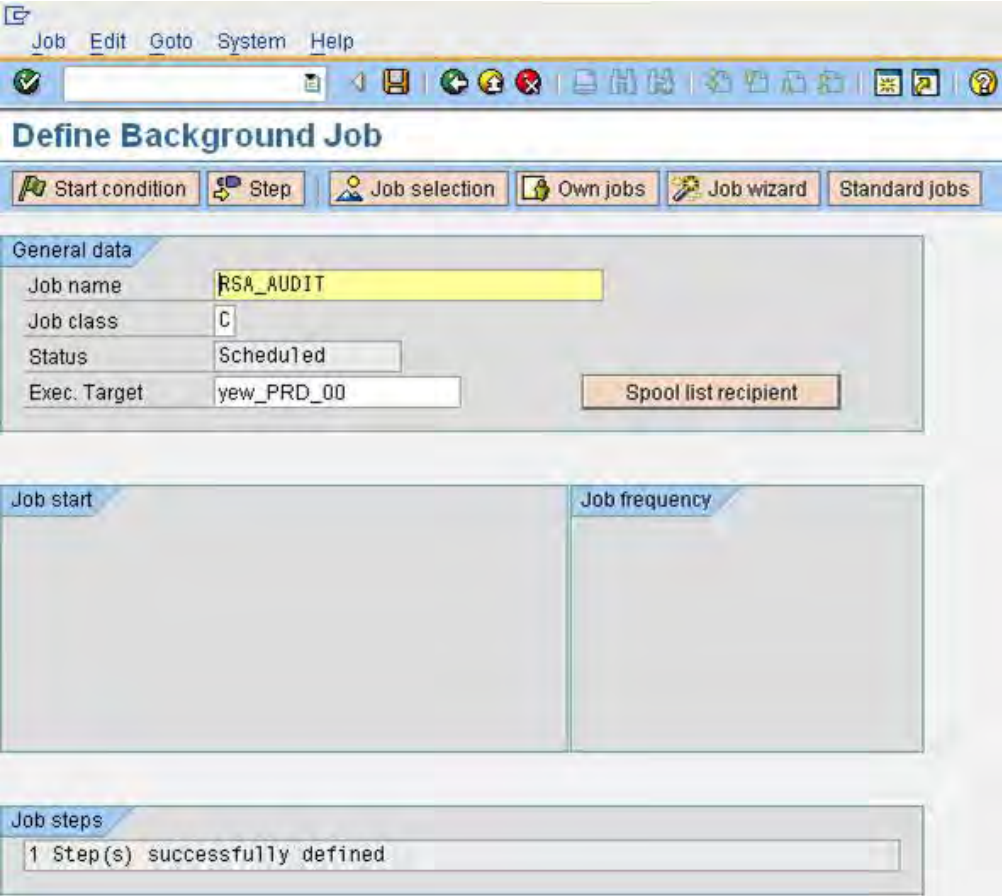
Scrn Assignm.

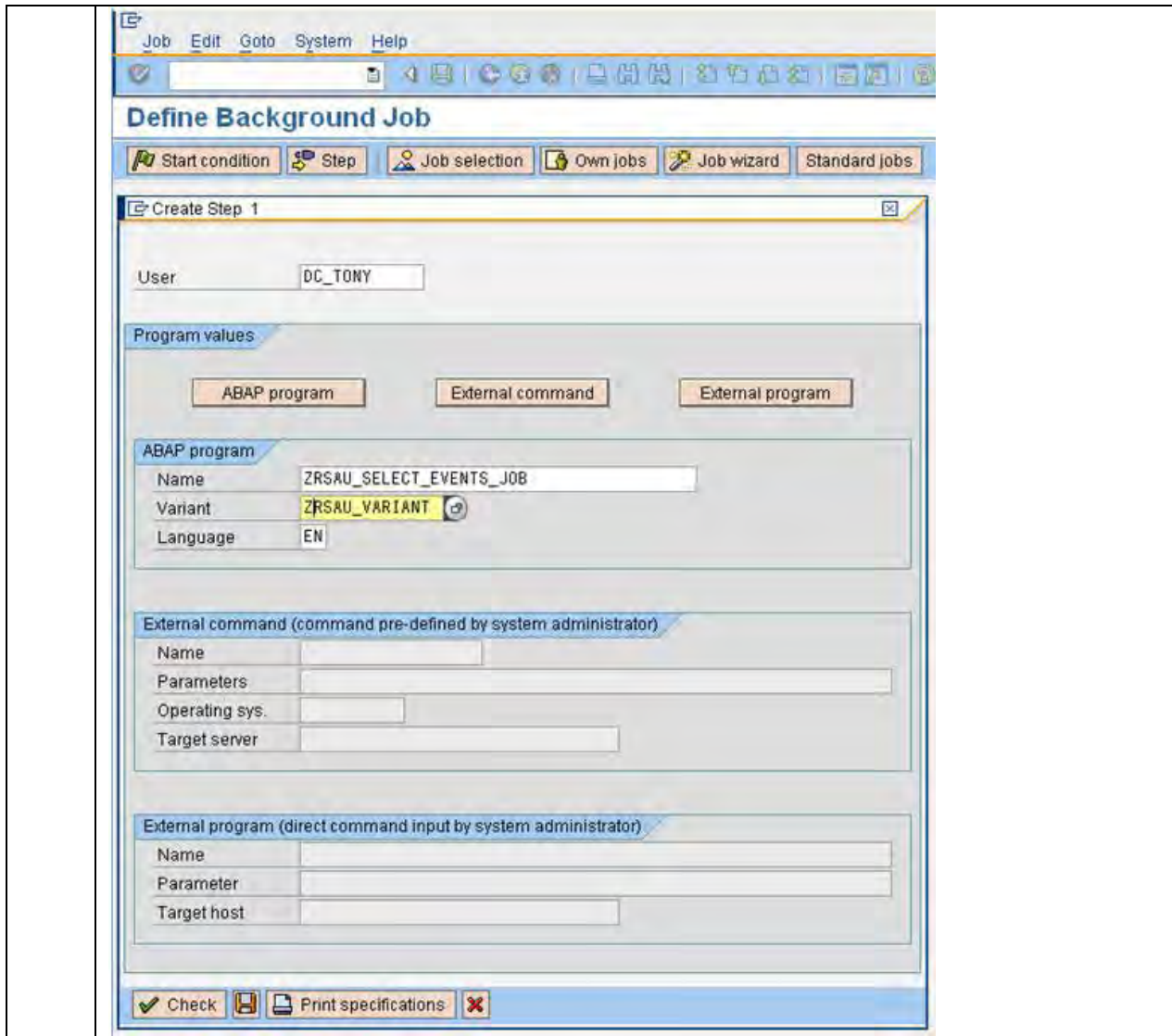
Created	Selection Scrms
<input checked="" type="checkbox"/>	1000

Objects for selection screen

Selection Scrms	Field name	Type	Protect field	Hide field	Hide field BIS	Save field without values	Switch GPA on	Required field
1.000	STRTDAT	P	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.000	STRTTIME	P	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.000	ENDDATE	P	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.000	ENDTIME	P	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.000	P FILE	P	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

7: Schedule a background job The following table shows the steps for scheduling a background job.



Step	Action
1	In the Command field, type <i>SM36</i> and press ENTER.
2	<p>In the Define Background Job window, do the following:</p> <ul style="list-style-type: none"> • In Job name, type <i>RSA_AUDIT</i> • In Job class, type <i>C</i> • Click Step <p>Note The SAP CI system will automatically populate the Status and Exec. Target fields.</p> 
3	<p>In the Create Step 1 dialog box, under ABAP program, do the following:</p> <ul style="list-style-type: none"> • In Name, type <i>ZRSAU_SELECT_EVENTS_JOB</i> • In Variant, type <i>ZRSAU_VARIANT</i> • Click Save

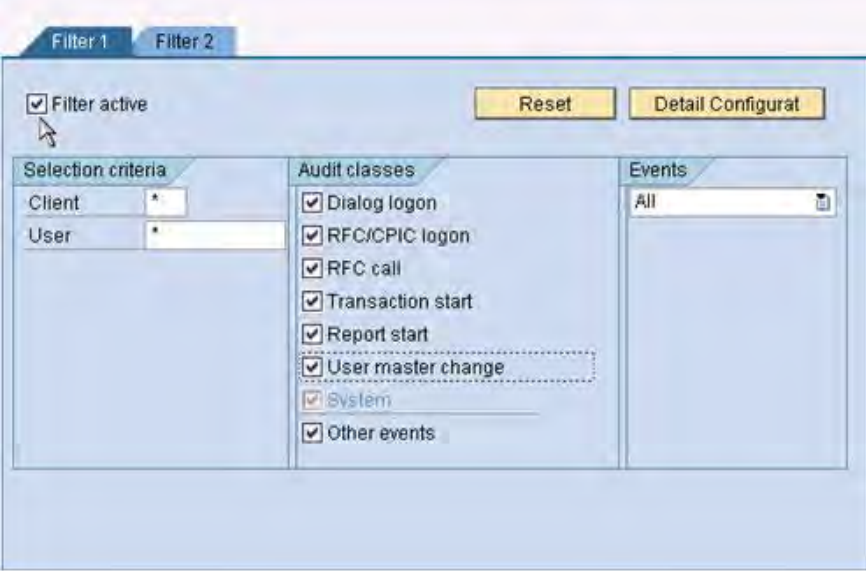



4	Close the dialog box and to return to the Define Background Job window, then click Start condition .
5	Click Date/Time .
6	In the Date/Time dialog box, do the following: a) In Required Date , type the date value b) In Time , type the time value c) Select the Periodic Jobs checkbox d) Select the Period Values checkbox e) Select the Other Period checkbox f) In Frequency , enter the value for how often you want to run the job
7	Click Save , then click Check to check for errors.
8	Click Activate .

8: Configure the SAP security audit

The following table shows the steps for configuring the SAP security audit.

Step	Action
1	To open the Security Audit window, in the Command field, type <i>SM19</i> and press ENTER.
2	<p>To create a new profile, click the New icon.</p> 
3	<p>In Profile name, type <i>TEST</i>.</p> <p>Note This is a customer-definable name.</p> 
4	Choose Filter 1 tab, then select Filter active checkbox and all audit classes that the customer requires.

	
5	Click Save .
6	<p>In the Confirmation Prompt popup window, click Yes to distribute configuration to all servers.</p> 
7	<p>Click Activate.</p> <p>The profile is now active for next system start.</p>
8	Restart the instance.

SAP logs

After the configuration is complete, customers can collect logs from the following systems within the SAP landscape:

- SAP Users
- SAP Transport
- SAP System Activity
- SAP Queue Activity
- SAP Audit Activity
- SAP Work Directory Activity
- SAP External Interface Activity

Demos for customers

After the configuration is complete, you can demonstrated the following:

- The RSA enVision job runs in the background.
 - The SAP system uses enVision to collect SAP and non-SAP logs from the landscape.
 - The SAP system creates the proper alerts in enVision based on predefined rules to show the customer, for example, system changes.
 - RSA enVision alerts the security admin personnel by email or text message. To demonstrate this process without an alert, use RSA enVision to show an alert for system change.
-

SAP system impact

Overview Since the SAP system collects the logs naturally, there is no additional system impact with the implementation of the solution. Instead, RSA enVision extracts the SAP system messages from the log directory and brings them into the enVision program.

Job run Since RSA enVision collects the SAP logs through a normal background job, you do not use any memory or CPU resources.

The ZRSAU_SELECT_EVENTS_JOB job runs and reads the logs from the SAP table in the work directory area and user table area, and from the transport logs and system log area. The SAP system creates all of these logs.

The background job simply reads and collects the logs, then makes a secure FTP call to upload the logs to RSA enVision. In order for the program to run, it will need the following SAP authorizations:

Event ID/MessageID (ID1)	Event Category Name	Event Category ID
000001	1401030000 User.Activity.Failed Logins	
000002	1401060000 User.Activity.Successful Logins	
000003	1402020400 User.Management.Users.Disabled	
000004	1401070000 User.Activity.Logoff	
000005	1401030000 User.Activity.Failed Logins	
000006	1605000000 System.Normal Conditions	
000007	1602010000 System.Accounting.Successful	
000008	1401060000 User.Activity.Successful Logins	
000009	1605020000 System.Normal Conditions.Services	
000010	1701000000 Config.Changes	
000011	1610000000 System.Startup	
000012	1612000000 System.Audit	
000013	1612000000 System.Audit	
000014	1602010000 System.Accounting.Successful	
000015	1602020000 System.Accounting.Errors	
000016	1402020300 User.Management.Users.Modifications	
000017	1402020400 User.Management.Users.Disabled	
000018	1402040100 User.Management.Password.Modification	

The job also collects logs for user activity.

**SAP
authorization**

You create a user for RSA enVision and use the following SAP authorization:

S_C_FUNCT
AUDIT_SET_INFO

You do not need to give full authorization; you can choose read/execute only under the activity.

Job scheduling

You can schedule the job based on the business environment. The job finishes very quickly, in only minutes.

Testing of SAP messages

Introduction to testing of SAP messages

EMC and RSA Labs verified that the SAP messages worked as expected and the logs were transferred successfully to enVision.

RSA enVision supports 8 categories of logs from SAP ECC. They are:

- Logon
- Other
- RFC call
- RFC logon
- Report start
- System
- Transaction start
- User master record

EnVision supports 23 separate formats of the listed log categories.

SAP messages Table 3 lists each message that was tested.

Table 3. SAP messages

Message ID	Description
000001 1401030000	User.Activity.Failed Logins
000002 1401060000	User.Activity.Successful Logins
000003 1402020400	User.Management.Users.Disabled
000004 1401070000	User.Activity.Logoff
000005 1401030000	User.Activity.Failed Logins
000006 1605000000	System.Normal Conditions
000007 1602010000	System.Accounting.Successful
000008 1401060000	User.Activity.Successful Logins
000009 1605020000	System.Normal Conditions.Services
000010 1701000000	Config.Changes
000011 1610000000	System.Startup
000012 1612000000	System.Audit
000013 1612000000	System.Audit
000014 1602010000	System.Accounting.Successful

000015 1602020000	System.Accounting.Errors
000016 1402020300	User.Management.Users.Modifications
000017 1402020400	User.Management.Users.Disabledent ID / MessageID (ID1) Event Category Name Event Category ID
000018 1402040100	User.Management.Password.Modification
000019 1402040197	RFC destination '&1', no authorization for func. group '&2'
000020 1402040198	RFC destination '&' has authorization for all needed function group
000021 1402040199	RFC destination '&' unfunctional (ping and authorization check done)
000022 1402040110	No suitable RFC Destination found in SDCCN settings
000023 1402040100	Connection to SAPNet refused
000024 1402040101	File has already been edited completely
000025 1402040102	Job already completed/cancelled
000026 1402040104	All selections deleted
000027 1402040105	Job(s) ended in the meantime

Conclusion

Summary

SAP landscapes produce numerous logs, and one log or combination of logs might be necessary to resolve problem for both production and non-production issues. Additionally, these logs are used on a day-to-day basis for change tracking, user-related information, and system activity.

RSA enVision has been extended to include a central repository, centralized log monitoring, and management capabilities throughout the SAP landscape. This enables SAP administrators to monitor access control in real-time. It also enables administrators to make changes to their SAP landscapes.

Next steps

To learn more about this and other solutions, contact an EMC representative or visit <http://www.emc.com>.
