RSA NetWitness Platform

Event Source Log Configuration Guide

SAP ERP Central Component

Last Modified: Monday, March 2, 2020

Event Source Product Information:

Vendor: SAP

Event Source: ERP Central Component (formerly R3 Enterprise)

Versions: 4.6 through 7.x

> **Note:** RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

Additional Downloads: zrsau_select_events_job.txt, sftpagent.conf.sap, nicsftpagent.conf.sap

> **Note:** Downloads are available from the RSA NetWitness Platform Event Source Downloads space using the following link: SAP ERP Central Component Downloads

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: sap

Collection Method: File

Event Source Class.Subclass: Host.Application Server

To configure the SAP ERP event source to work with RSA NetWitness Platform, you must complete these tasks:

I. Configure SAP ERP Central Component

II. Set up the SFTP Agent and NetWitness Log Collector

Configure SAP ERP Central Component

Perform the following tasks to configure SAP ERP Central Component:

I. Change SAP Configuration

II. Create the ZRSA Table

III. Create ZRSAU_AS Table

IV. Create Message Class ZRSA

V. Activate the SAP Logs Trigger

VI. Create ZRSAU_SELECT_EVENTS_JOB

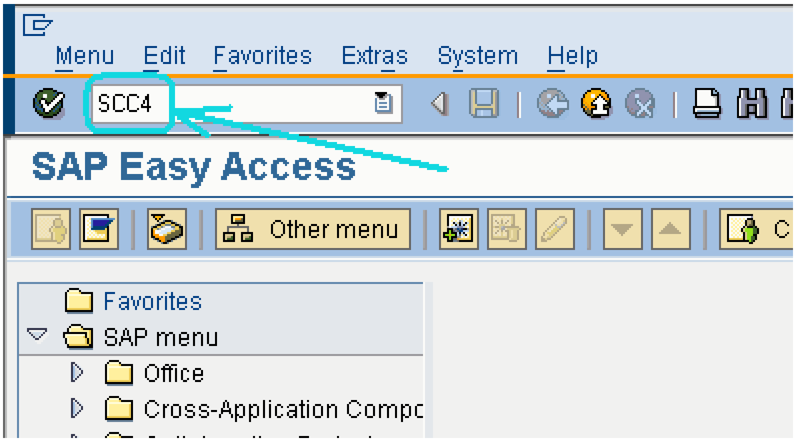
VII. Create a Variant for Job Scheduling

VIII. Schedule Background Job

Task I: Change SAP Configuration

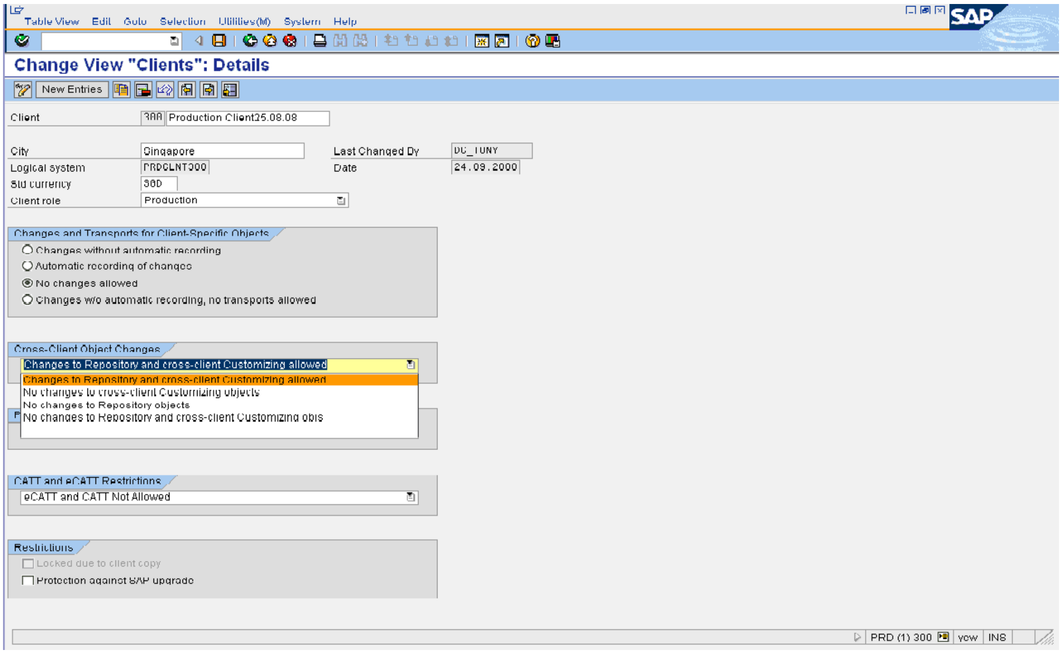
To change the SAP configuration:

1. Log on to SAP using the appropriate user account.
2. In the transaction field below the toolbar, type **SCC4**.



3. From the **Cross-Client Object Changes** list, select **Changes to Repository and**

cross-client Customizing allowed.



Change View "Clients": Details

Client	300 Production Client25.08.08		
City	Singapore	Last Changed By	DC_TONY
Logical system	PRDCLNT300	Date	24.09.2000
Std currency	SGD		
Client role	Production		

Changes and Transports for Client-Specific Objects

○ Changes without automatic recording
○ Automatic recording of changes
● No changes allowed
○ Changes w/o automatic recording, no transports allowed

Cross-Client Object Changes

Changes to Repository and cross-client Customizing allowed

Changes to Repository and cross-client Customizing allowed
No changes to cross-client Customizing objects
No changes to Repository objects
No changes to Repository and cross-client Customizing objs

CATT and eCATT Restrictions

eCATT and CATT Not Allowed

Restrictions

□ Locked due to client copy
□ Protection against SAP upgrade

Task II: Create the ZRSA Table

To create the ZRSA database table:

1. Enter **SE11** for the transaction code to create a new database table.
2. In the **Database table** field, enter **ZRSA**, and click **Create**.
3. In the **Short Description** field, enter a description of the table.
4. In the **Delivery and Maintenance** tab, do the following:
   a. In the **Delivery Class** field, type **A** (for Application table).
   b. From the **Data Browser/Table View Maint.**list, select **Display/Maintenance Allowed with Restrictions**.
5. Click the **Fields** tab, and enter information for the table fields as shown.

Field	Key	Initial Values	Data Element	Data Type	Length	Description
MANDT	Select	Select	MANDT	CLNT	3	Client

Field	Key	Initial Values	Data Element	Data Type	Length	Description
TODATE			DATUM	DATS	8	Date
TOTIME			TIME	CHAR	6	Time in CHAR format

6. Click **Save**.
7. In the Create Object Directory Entry window, in the Package field, enter **$TMP** and click **Save**.
8. Click **Activate**.
9. Click **Technical Settings** and set the following parameters:
   - In the **Data class** field, select **APPL0**.
   - In the **Size category** field, select **0**.
   - In the **Buffering** section, select **Buffering not allowed**.
10. Click **Activate**

Task III: Create the ZRSAU_AS Table

To create the ZRSAU_AS database table:

1. Enter **SE11** for the transaction code to create a new database table.
2. In the **Database table** field, enter **ZRSAU_AS** and click **Create**.
3. In the **Short Description** field, enter a description of the table.
4. In the **Delivery and Maintenance** tab, fill in the fields as follows:
   a. In the **Delivery Class** field, type **A** (for Application table).
   b. From the **Data Browser/Table View Maint.**list, select **Display/Maintenance Allowed with Restrictions**.
5. Click the **Fields** tab, and enter information for the table fields as shown.

Field	Key	Initial Values	Data Element	Data Type	Length	Description
DSET	Select	Select	EDIUOLDDIR	CHAR	100	Pathname and directory of source file
CHGDATE			DATUM	DATS	8	Date
CHGTIME			TIME	CHAR	6	Time in CHAR format
ARCHFLAG			FLAG	CHAR	1	General Flag

6. Click **Save**.
7. In the Create Object Directory Entry window, in the Package field, enter **$TMP** and click **Save**.
8. Click **Activate**.

Task IV: Create Message Class ZRSA

You must create a message class to display messages in the ZRSAU_SELECT_EVENTS_JOB program.

To create the ZRSA message class:

1. Enter **SE91** for the transaction code.
2. In the **Message Class** field, enter **ZRSA**.
3. In the Create Object Directory Entry window, in the Package field, enter **$TMP** and click **Save**.

4. Click the **Messages** tab, and enter the information for the table fields as shown:

Message	Message Short Text
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**.

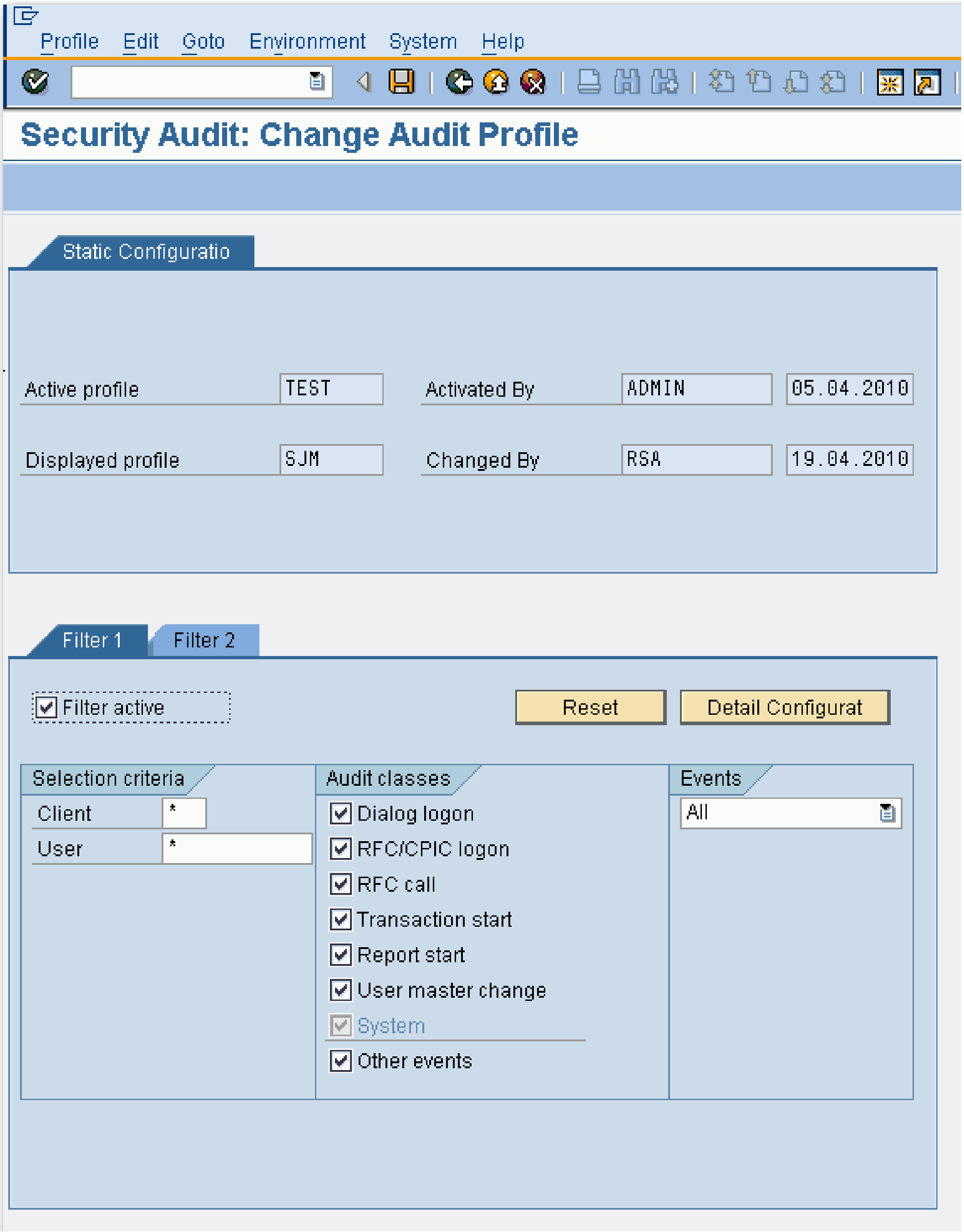
Task V: Activate the SAP Logs Trigger

To activate the SAP logs trigger:

1. Enter **SM19** for the transaction code to create the object.
2. Click **Create** to create a profile.
3. Enter a name for the profile. and click **Continue**.
4. In the **Filter 1** tab, set the following:
    a. In the **Audit Classes** section, select all available options.

    b. In the **Events** section, select **All**.

c. Select **Filter Active**



Security Audit: Change Audit Profile

Active profile	TEST	Activated By	ADMIN	05.04.2010
Displayed profile	SJM	Changed By	RSA	19.04.2010

☑ Filter active

Selection criteria

Client	*
User	*

Audit classes

☑ Dialog logon
☑ RFC/CPIC logon
☑ RFC call
☑ Transaction start
☑ Report start
☑ User master change
☑ System
☑ Other events

Events

All

5. Click **Display <-> Change**, or press F6.

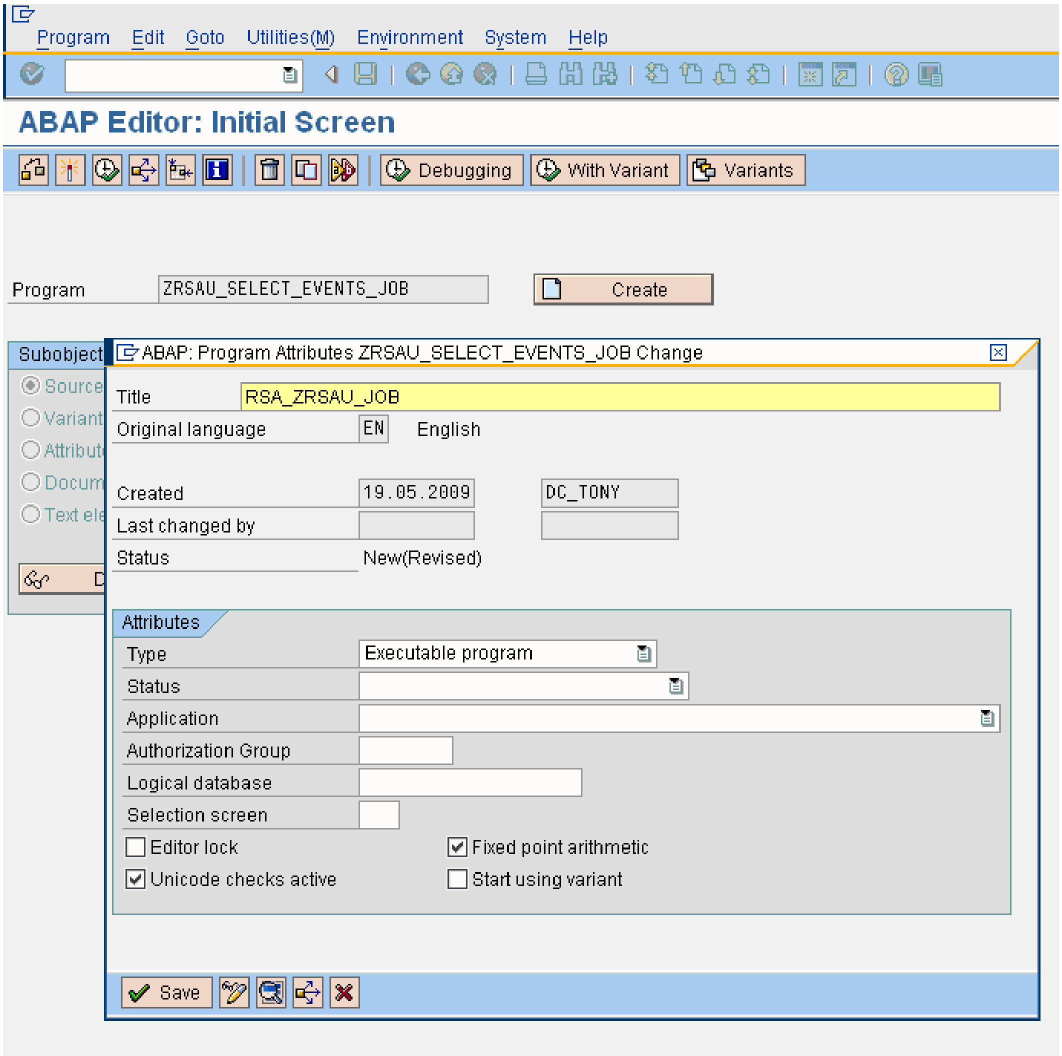
6. When prompted to confirm the changes, click **Yes**.

7. Click **Activate**.

Task VI: Create ZRSAU_SELECT_EVENTS_JOB

To create ZRSAU_SELECT_EVENTS_JOB:

1. Enter **SE38** for the transaction code to create the object.
2. For the program name, type **ZRSAU_SELECT_EVENTS_JOB**, and click **Create**.
3. In the **Program** field, type **ZRSAU_SELECT_EVENTS_JOB**.
4. From the **Type** list, select **Executable Program**.



Program: ZRSAU_SELECT_EVENTS_JOB

ABAP: Program Attributes ZRSAU_SELECT_EVENTS_JOB Change

Title: RSA_ZRSAU_JOB

Original language: EN English

Created: 19.05.2009 DC_TONY

Last changed by:

Status: New(Revised)

Attributes

Type: Executable program

Status:

Application:

Authorization Group:

Logical database:

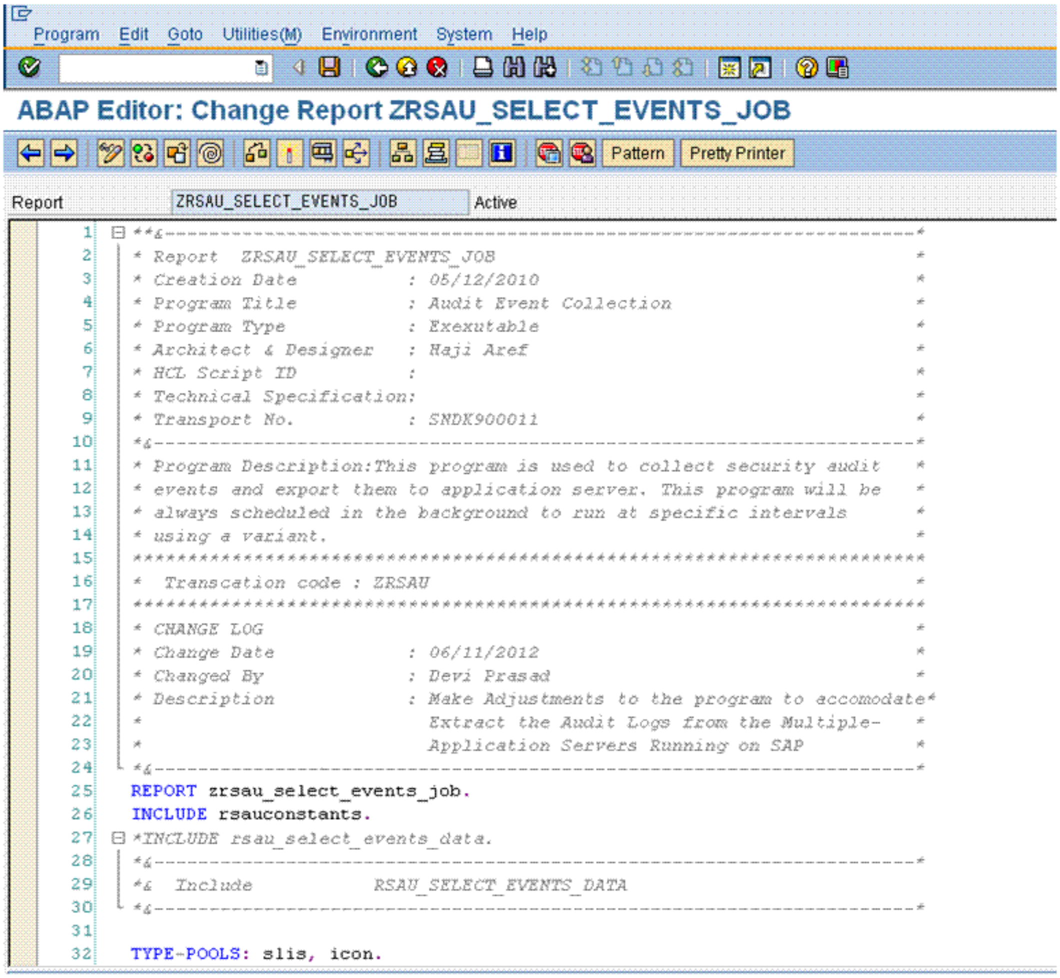
Selection screen:

☐ Editor lock ☑ Fixed point arithmetic

☑ Unicode checks active ☐ Start using variant

5. Click **Save**.

6. In the Create Object Directory Entry window, in the Package field, enter **$TMP** and click **Save**.
7. Click **Save**.
8. Copy the contents from the **ZRSAU_SELECT_EVENTS_JOB** script provided by RSA to the ABAP Editor.
9. Click **Save**, and check for any errors.
10. Click **Activate**.



ABAP Editor: Change Report ZRSAU_SELECT_EVENTS_JOB

Report ZRSAU_SELECT_EVENTS_JOB Active

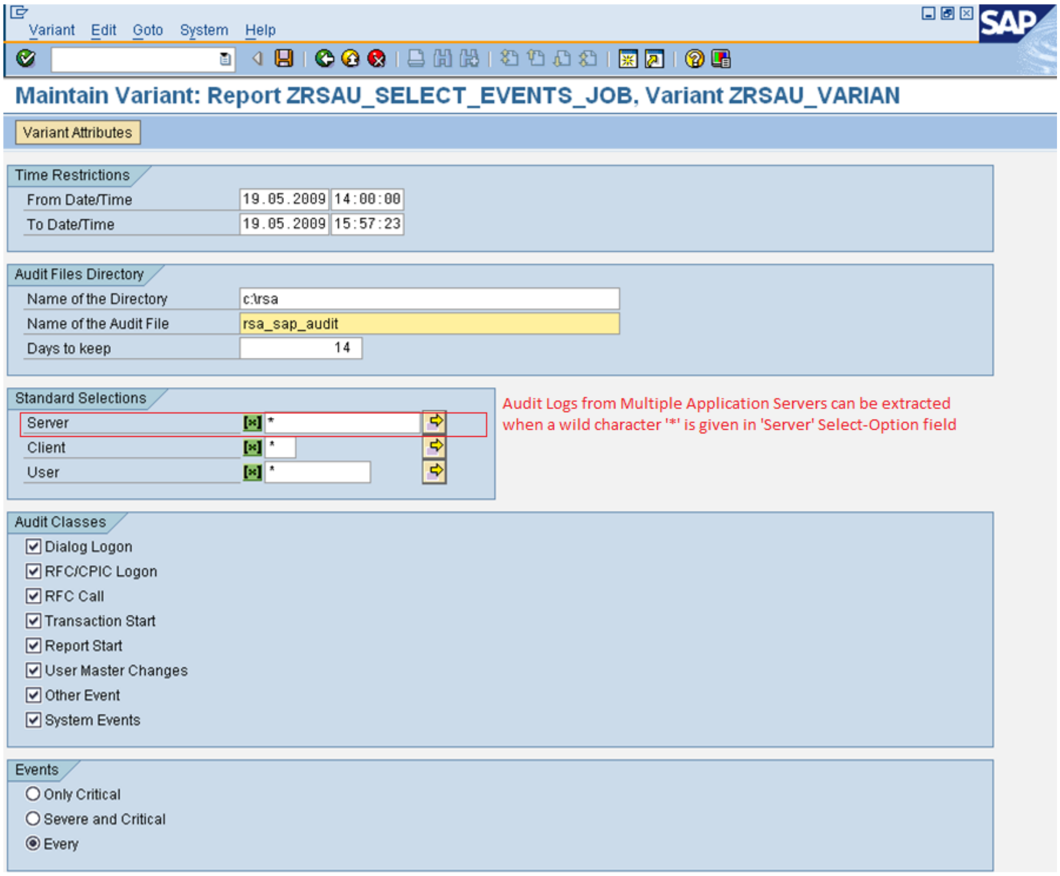
```
**&---------------------------------------------------------------------*
* Report  ZRSAU_SELECT_EVENTS_JOB                                       *
* Creation Date            : 05/12/2010                                 *
* Program Title            : Audit Event Collection                     *
* Program Type             : Exexutable                                 *
* Architect & Designer     : Haji Aref                                  *
* HCL Script ID            :                                            *
* Technical Specification:                                              *
* Transport No.            : SNDK900011                                 *
*&----------------------------------------------------------------------*
* Program Description:This program is used to collect security audit    *
* events and export them to application server. This program will be    *
* always scheduled in the background to run at specific intervals       *
* using a variant.                                                      *
*************************************************************************
*  Transcation code : ZRSAU                                             *
*************************************************************************
* CHANGE LOG                                                            *
* Change Date              : 06/11/2012                                 *
* Changed By               : Devi Prasad                                *
* Description              : Make Adjustments to the program to accomodate*
*                            Extract the Audit Logs from the Multiple-  *
*                            Application Servers Running on SAP         *
*&----------------------------------------------------------------------*
REPORT zrsau_select_events_job.
INCLUDE rsauconstants.
*INCLUDE rsau_select_events_data.
*&----------------------------------------------------------------------*
*&  Include           RSAU_SELECT_EVENTS_DATA
*&----------------------------------------------------------------------*

TYPE-POOLS: slis, icon.
```

Task VII: Create a Variant for Job Scheduling

To create a variant for job scheduling:

1. Enter **SE38** for the transaction code to create the object.
2. In the **Program** field, type **ZRSAU_SELECT_EVENTS_JOB**.
3. In the toolbar, select **Variants** or press CTRL+F1.
4. In the Variant field, type **ZRSAU_VARIANT**, and click **Create**.
5. Specify the following information for the variant:
   - In the **From Date/Time**, **To Date/Time**, **Name of the Directory**, **Name of the Audit File** and **Days to keep** fields, enter appropriate values.
   - Under **Audit Classes**, select all options.
   - Under Events, select **Every**.



Maintain Variant: Report ZRSAU_SELECT_EVENTS_JOB, Variant ZRSAU_VARIAN

Time Restrictions

From Date/Time 19.05.2009 14:00:00

To Date/Time 19.05.2009 15:57:23

Audit Files Directory

Name of the Directory c:\rsa

Name of the Audit File rsa_sap_audit

Days to keep 14

Standard Selections

Server *

Client *

User *

Audit Logs from Multiple Application Servers can be extracted when a wild character '*' is given in 'Server' Select-Option field

Audit Classes

☑ Dialog Logon
☑ RFC/CPIC Logon
☑ RFC Call
☑ Transaction Start
☑ Report Start
☑ User Master Changes
☑ Other Event
☑ System Events

Events

○ Only Critical
○ Severe and Critical
● Every

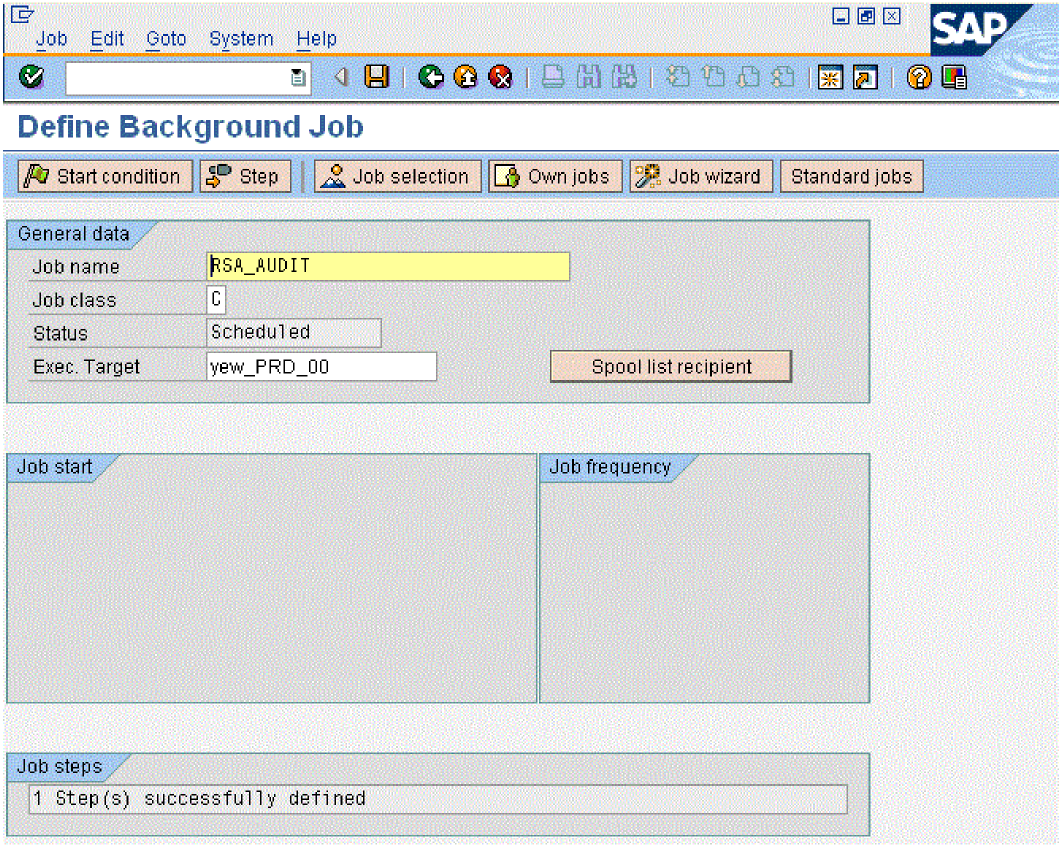
6. Click **Save**.
7. In the **Meaning** field, type **variant**.
8. Select the **Only for Background Processing** option, and click **Save**.

Task VIII: Schedule Background Job

This background job runs at the frequency that you specify. The system downloads events to the directory specified in the program of the application server and inserts the date and time stamp as a prefix to the filename extension.

To schedule the background job:

1. Enter **SM36** for the transaction code.
2. Under **General Data**, do the following:
   a. In the **Job Name** field, type **RSA_AUDIT**.
   b. In the **Job Class** field, type **C**.
   c. In the **Exec. Target** field, choose the appropriate profile name.
3. To define the job steps, click **Step**.



Define Background Job

General data

Job name RSA_AUDIT

Job class C

Status Scheduled

Exec. Target yew_PRD_00

Job start

Job frequency

Job steps

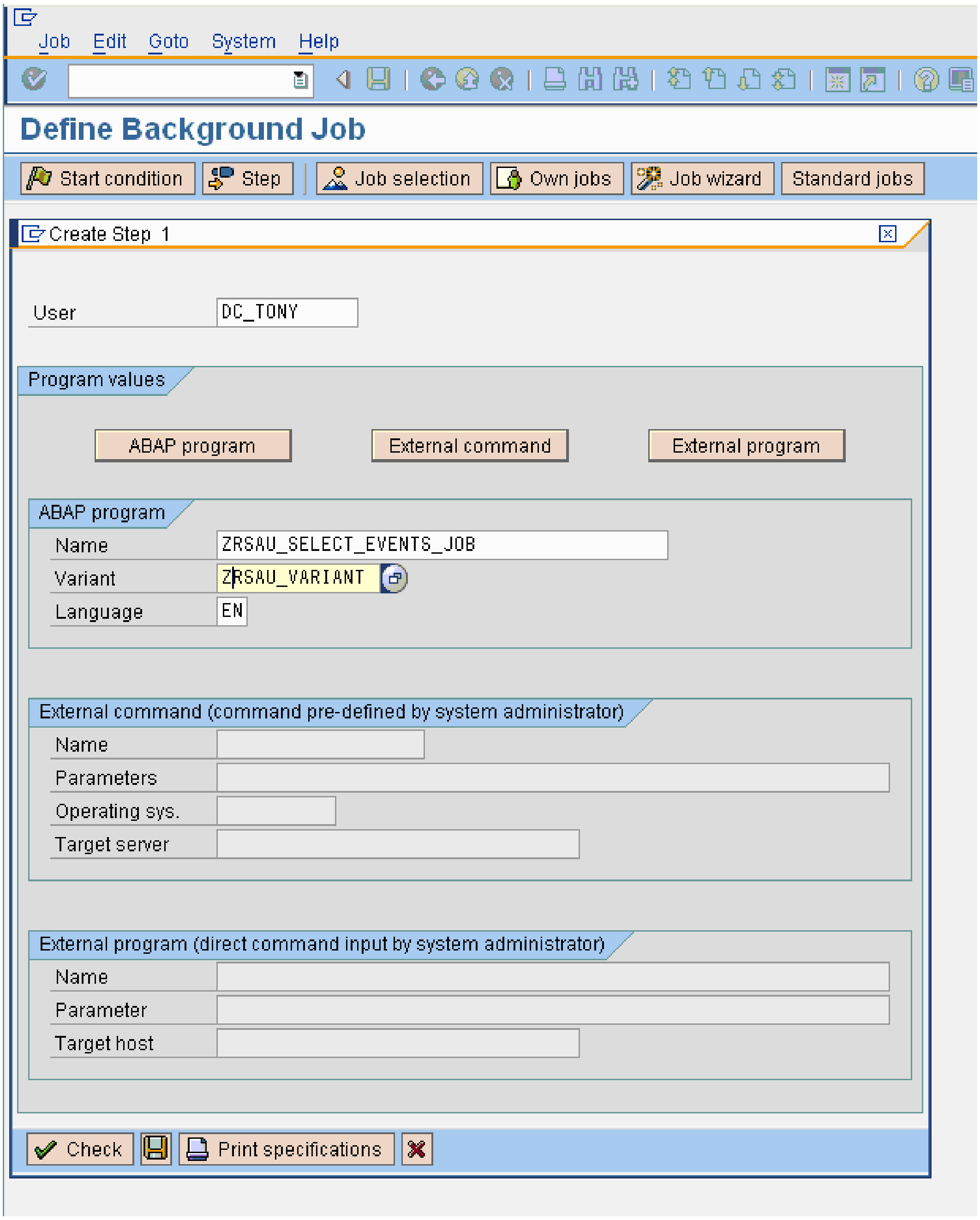
1 Step(s) successfully defined

4. In the **ABAP program** area, do the following:

   a. In the **Name** field, type **ZRSAU_SELECT_EVENTS_JOB**.

   b. In the **Variant** filed, type **ZRSAU_VARIANT**.

5. Click **Save**.



Define Background Job

Create Step 1

User DC_TONY

Program values

ABAP program

Name ZRSAU_SELECT_EVENTS_JOB

Variant ZRSAU_VARIANT

Language EN

External command (command pre-defined by system administrator)

Name

Parameters

Operating sys.

Target server

External program (direct command input by system administrator)

Name

Parameter

Target host

6. Go back to the previous screen.
7. Click **Start Condition**.
8. Click **Date/Time**.
9. In the **Required Date** and **Time** fields, enter appropriate values, and select **Periodic Jobs**.
10. Click **Period Values**.

11. Click **Other Period**.
12. Assign the value for the frequency to run the job.
13. Click **Save**.
14. Click **Check** to check for inconsistencies.

Set Up SFTP Agent and NetWitness Log Collector

To configure RSA NetWitness Platform, set up the SFTP Agent and configure the Log Collector for file collection.

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SFTP Shell Script File Transfer

Configure the Log Collector for File Collection

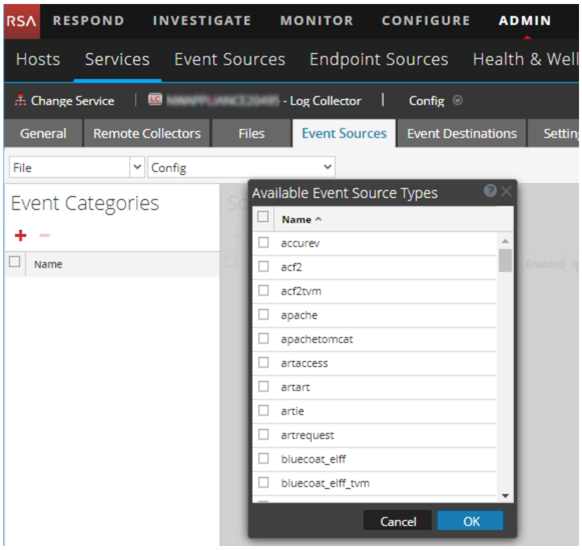
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **File/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.

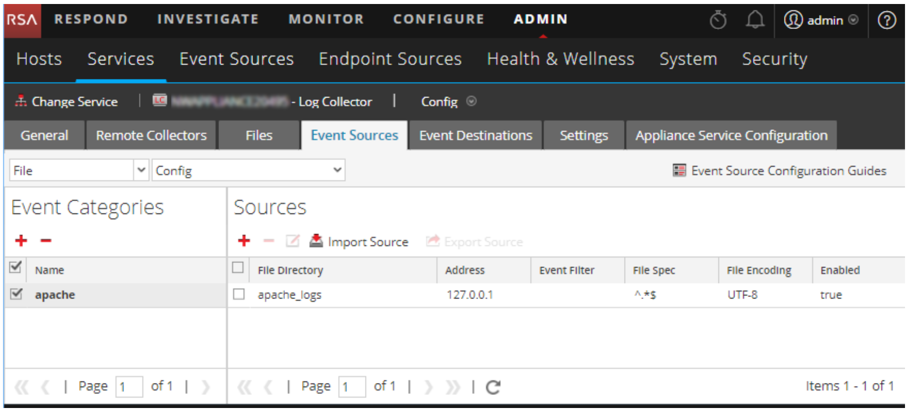


5. Select the correct type from the list, and click **OK**.

   Select **sap** from the **Available Event Source Types** dialog.

   The newly added event source type is displayed in the Event Categories panel.

   > **Note:** The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



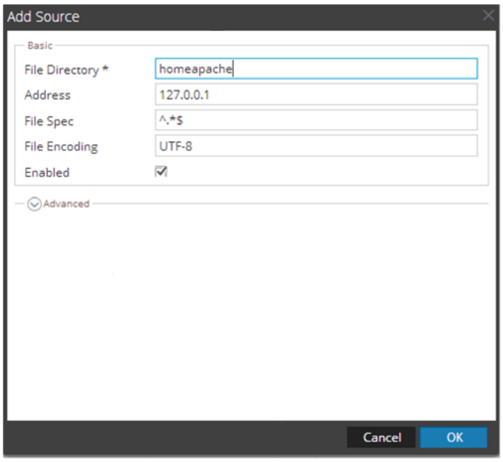
☑	Name
☑	apache

□	File Directory	Address	Event Filter	File Spec	File Encoding	Enabled
□	apache_logs	127.0.0.1		^.*$	UTF-8	true

6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.

> **Note:** Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

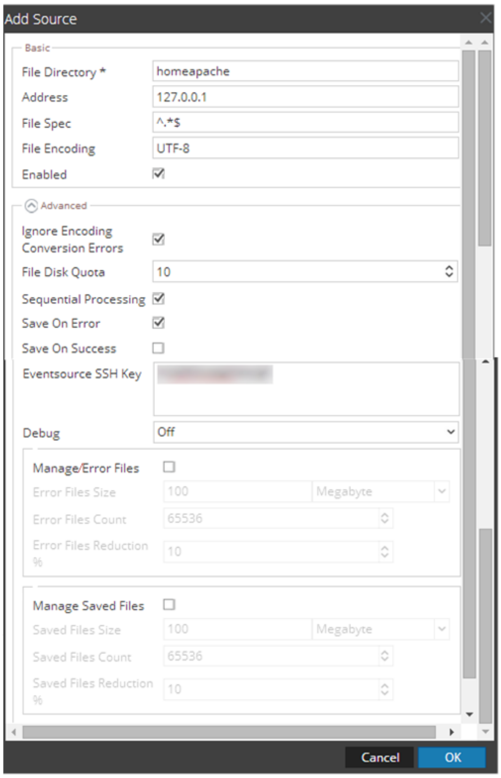


Add Source

Basic

File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑

Advanced



Add Source

Basic

File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑

Advanced

Ignore Encoding Conversion Errors ☑
File Disk Quota 10
Sequential Processing ☑
Save On Error ☑
Save On Success ☐
Eventsource SSH Key [redacted]
Debug Off

Manage/Error Files ☐
Error Files Size 100 Megabyte
Error Files Count 65536
Error Files Reduction % 10

Manage Saved Files ☐
Saved Files Size 100 Megabyte
Saved Files Count 65536
Saved Files Reduction % 10

7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.

8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.