

HowTo

Configuration of the VSA with SAP NetWeaver 2004(s) ABAP



Avira Support
August 2009



Content

SAP System Requirements	3
SAP Platforms.....	3
OS System Requirements.....	3
Important Transactions	3
What should be considered?	4
How is the VSA connected to the SAP system (ABAP)?	5
How to define a new RFC destination with TCP/IP	5
Definition of an RFC Destination.....	6
This transaction 'spro' is the way to the system administration of the Netweaver...	7
Definition of a virus scanner group.....	8
Definition of a Virus Scan Adapter or Server.....	9
Definition for profiles which control the activation of the VSA	12
Definition of the Steps in the Virus Scan Profile.....	14
Testing the installation of the Virus Scan Server (Profile Z_AVIRA).....	16
Trace possibilities in the SAP system.....	18
Activation of the Active Content Scanning.....	21
Testing the Installation of the Virus Scan Server (profile ZACTIVECONTENT).....	25
Integration of the VSA without RFC destination.....	26
Environment variables VSA_LIB and VSA_DEBUG.....	27
Application server or self-starter	27
External activation of the AntiVir VSA via VSCAN_RFC (self-starter)	28
Scan of SAR and CAR archives	29



SAP System Requirements

SAP Platforms

SAP NetWeaver 6.40 with support package 7 or more; for the ABAP engine with SAP-BASIS 640 support package 11 or more;
for the J2EE engine with support package 13 or more SAP NetWeaver 2004s (7.0)

OS System Requirements

Operating systems Linux/Unix (32-bit/64-bit):

Red Hat Enterprise Linux 5 Server; Red Hat Enterprise Linux 4 Server; Novell SUSE Linux Enterprise Server 10 - 10.2; Novell SUSE Linux Enterprise Server 9; Debian GNU/Linux 4 (stable); Ubuntu Server Edition 8; Sun Solaris SPARC 9; Sun Solaris SPARC 10

Operating systems Windows (for 32-bit only):

Windows 2000 Server, SP4 recommended
Windows 2000 Advanced Server, SP4 recommended
Windows 2003 Server
Windows Server 2008 (not for Core-Setup)

Important Transactions

Transactions:

sm59	→	Configuration of the RFC connection
spro	→	System administration of the SAP Netweaver
vscan	→	Virus Scan Provider Definition
vscantrace	→	directed Trace in case of virus attack
vscanprofile	→	direct access to the definition of the virus scan profiles in the SAP system
vscangroup	→	direct access to the definition of the virus scan groups in the SAP system
vscantest	→	Test for the virus scan interface



What should be considered?

Important information about the specific configuration of ABAP:

For the installation of the RFC connection it is important that the name of the RFC destination begins with "VSCAN_". The virus scanner can only work with this beginning of the name.

In the menu "Technical settings -> program ID" the RFC destination has to be entered again.

The option "Registered server program" has to be chosen as kind of activation for the RFC destination.

The procedure is valid for the virus scan server via RFC destination.



How is the VSA connected to the SAP system (ABAP)?

How to define a new RFC destination with TCP/IP

Transaction SM59

RFC Connections	Type	Comment
ABAP Connections	3	
HTTP Connections to External Server	G	
Internal Connections	I	
SNA/CFP-C connections	S	
TCP/IP connections	T	
CALLTP_WindowsNT	T	Transport Tools: tp Interface "generated"
DOCUMENTATION_HELP	T	Call WinHelp and WinWord from R/3
EU_SCRP_WN32	T	Graphical Screen Painter (WindowsNT / Windows95)
F1_HELP_SERVER	T	Windows RFC server for F1 help on fields, messages and command fields
F1_HELP_SERVER_32	T	Windows RFC server for F1 help on fields, messages and command fields
F1_HELP_SERVER_40	T	Windows RFC server for F1 help on fields, messages and command fields
IGS_RFC_DEST	T	Generated RFC destination for IGS
LOCAL_EXEC	T	Starts the Program 'RFCEXC' on Front End Machine
LOCAL_PRINT	T	Runs rfexec for X terminals
MDX_PARSER	T	MDX Parser for ODBO BAPI
R3_WINDOWS_SERVER	T	Desktop integration for Windows (WinWord 6.0)
SDB_SESSION	T	SDB command mode dbmrfc
SAPFORMS	T	RFC server for executing a work item using a form
SAPGUI	T	SAPGUI
SAPHTTPA	T	Automatically Generated on 19991205
SAPIRCONTROLLER	T	Information Repository Controller
SAPIRPCFILETRANSFER	T	IR - PC FileTransfer RFC Server
SAPJ2EE	T	
SAPKPROTP	T	Generated automatically on 20040325
SAP_SCHEDULE_16	T	Date calendar update front-end
SAP_SCHEDULE_32	T	Starts the update calendar sapkale.exe for the 32-bit GUI
SAP_SSFATGUI	T	SSF on the SAPgui machine
SERVER_EXEC	T	Starts Program 'RFCEXC' on Application Server
SLD_NUC	T	Automatically generated for System Landscape Directory (SLD)
SLD_UC	T	Automatically generated for System Landscape Directory (SLD)
VFOLDER	T	Virtual folder for AL
VSCAN_AVIRA_WIN	T	
Connections via ABAP Driver	X	



Definition of an RFC Destination

Transaction SM59

The screenshot shows the SAP SM59 transaction interface. The title bar indicates the transaction is 'RFC Destination VSCAN_AVIRA_WIN'. The main window is divided into several sections:

- Connection Test** and **Unicode Test** buttons are visible at the top.
- RFC Destination** is set to 'VSCAN_AVIRA_WIN'.
- Connection Type** is 'T' (TCP/IP Connection).
- Description** fields: Description 1 is 'Avira AntiVir VSA', Description 2 is empty, and Description 3 is empty.
- Administration** tab is selected, showing:
 - Activation Type**: Registered Server Program.
 - Registered Server Program**: Program ID is 'VSCAN_AVIRA_WIN'.
 - Start Type of External Program**: Default Gateway Value.
 - CPI-C Timeout**: Specify Timeout, with a value of '20'.
 - Gateway Options**: Gateway Host is 'vmserv1' and Gateway service is 'sapgw00'.

- ▶ Create an RFC connection of the type *T* in transaction SM59

You have to use the following name convention for the configuration of the scan server:

- VSCAN_<Hostname>, in case you want to start only one virus scan server on the host
- VSCAN_<Hostname>-<Number>, in case you want to start several virus scan servers on the host.

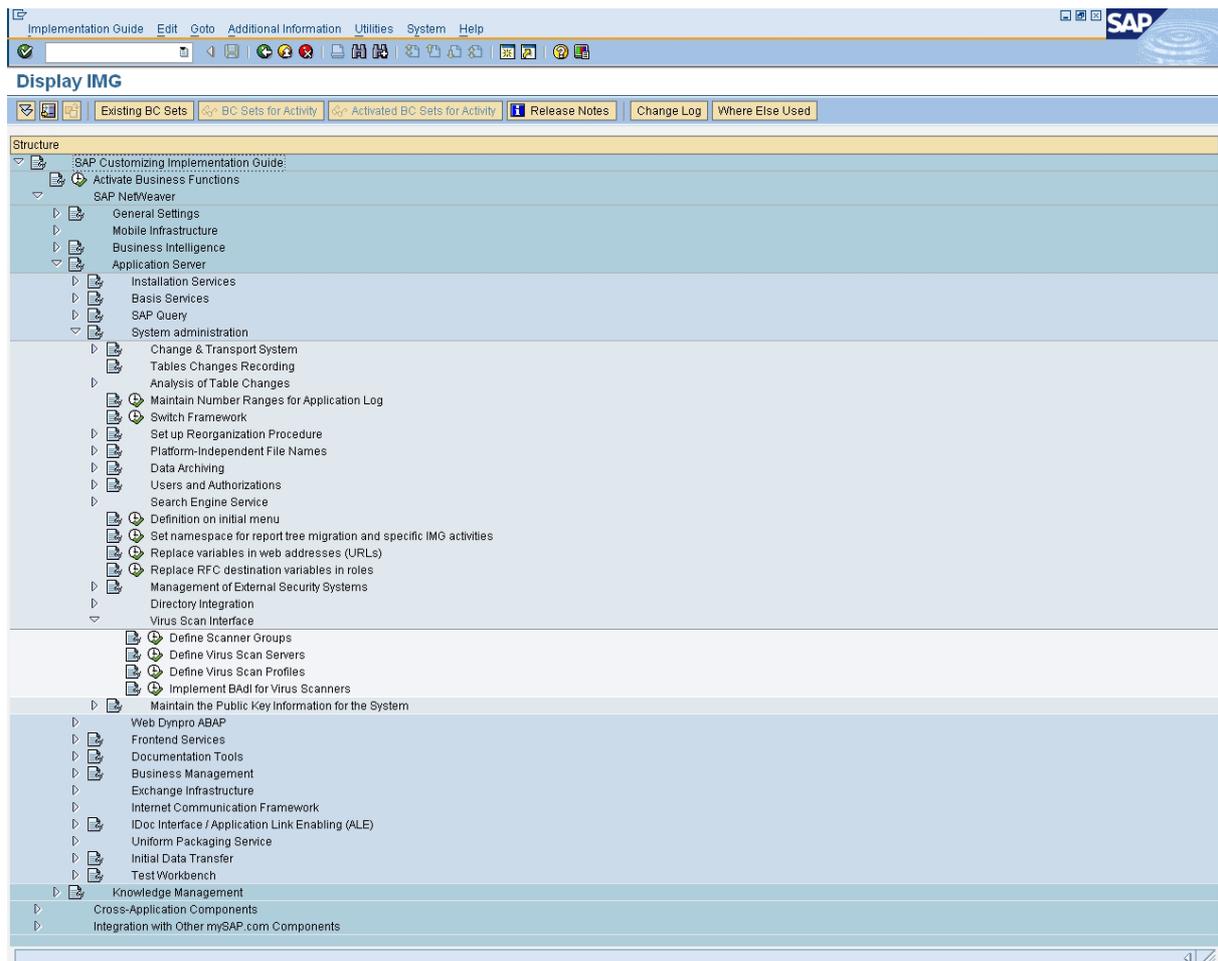
The figure is serially numbered and separated by a hyphen from the host name. Possible names are: VSCAN_HOST123, VSCAN_HOST345-1, VSCAN_HOST345-2 etc.



- ▶ Choose the kind of activation “Registered server program”.
- ▶ Use the name of the RFC destination as program ID.
- ▶ Enter the address of the system gateway as gateway host and gateway service.
In case you start the virus scan server via the computing center management system on an application server, choose the gateway of this application server.

This transaction ‘spro’ is the way to the system administration of the Netweaver

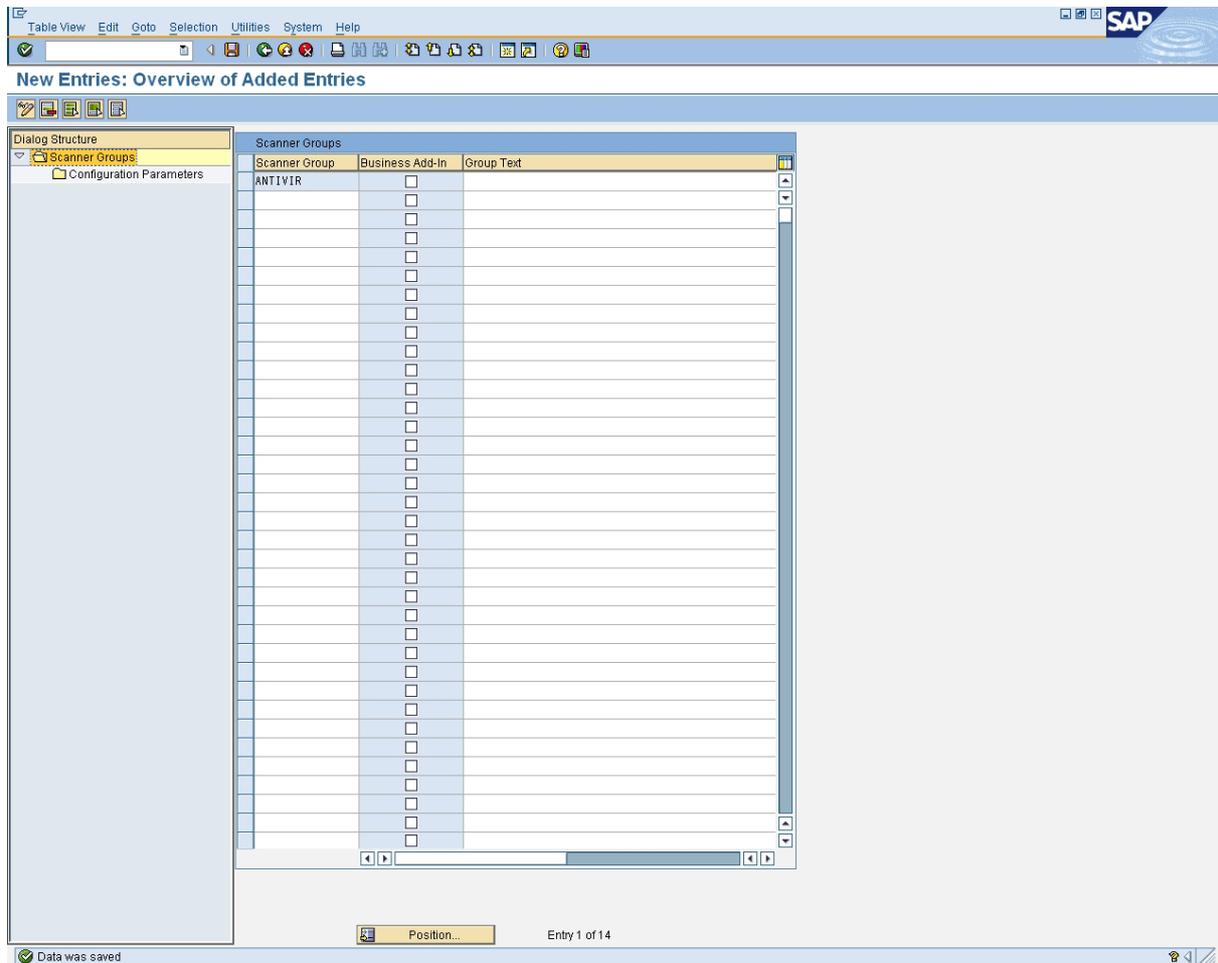
- Virus scanner group
- Virus scan server
- Virus scan profile





Definition of a virus scanner group

► Transaction 'vscangroup'



Choose new entries.

You get to the menu new entries: Overview of added entries.
Enter the data for the definition of the scanner group.

Scanner group: Freely definable name of the scanner group.

Business add-in: If this indicator is set, the program transfers the request for a virus scan instance for this scanner group to the Business Add-In VSCAN_INSTANCE, with which customers can include their own virus scanners. If this option is not set, the program searches for a suitable virus scan server among the set of virus scan servers maintained in *Customizing* that have this scanner group.

Group text: Explanations about the scanner group.



Definition of a Virus Scan Adapter or Server

Transaction 'vscan'

Provider type choice:

The screenshot shows the SAP 'vscan' transaction interface. At the top, there is a menu bar with options: Table View, Edit, Goto, Selection, Utilities, System, Help. Below the menu is a toolbar with various icons. The main area is titled 'New Entries: Details of Added Entries'. It contains a table with the following data:

Provider Type	ADAPTER (Virus Scan Adapter)
Provider Name	ADAPTER (Virus Scan Adapter)
Status	SERVER (Virus Scan Server)

Below the table is a 'Virus Scan Provider Definition' section with the following fields:

- Scanner Group:
- Status: Active (Application Server)
- Server: IKVM2K3SP2SAP_NSP_00
- Reinit. Interv.: Hours
- Adapter Path: E:\VSA\antivirsa.dll

ADAPTER (Virus Scan Adapter):

This option can be chosen in case Avira GmbH supports the SAP operation system directly. The virus scanner runs directly in the SAP web application server and no files have to be sent to an outsourced server via the network. With this configuration, there is no need to set a **VCSAN RFC** as the SAP system communicates directly with the virus scanner.



SERVER (Virus Scan Server):

This option has to be activated if Avira does not support the SAP operation system. The files which have to be scanned are sent to an outsourced server. After the scan the virus scanner informs the SAP system if a virus has been found or not. The further handling of the upload is done by the SAP virus scan interface.

The example underneath shows the configuration with the outsourced server.

- ▶ Choose in the IMG *SAP Web Application Server/ System administration/ virus scan interface*
- ▶ Choose the *Execute* option next to *Define Virus Scan Servers*.
The screen *View: Change "Virus Scan Servers": Overview* appears.
- ▶ Choose *New Entries*.
The screen *New Entries: Details of Added Entries* appears.
- ▶ Enter the name of the virus scan server into the box *Scan server*. The name has to be the same as the name of the RFC destination which contains the technical connection to the virus scan server.



Table View Edit Goto Selection Utilities System Help SAP

Display View "Virus Scan Provider Definition": Details

Provider Type: SERVER (Virus Scan Server)
 Provider Name: VSCAN_AVIRA_WIN
 Status: ■ Start Stop

Virus Scan Provider Definition

Scanner Group	ANTIVIR	Instance Name	
Status	Active (Application Server)	Max. Instances	8
Server	IKVM2K3SP2SAP_NSP_00	Code Page	1100
Trace Level	Errors Only	Reinit. Interv.	24 Hours
Adapter Path	E:\VSA\antivirvsa.dll	Last Initialization:	12.10.2009 14:14:05
Configuration			Local

Engine Data

Version	7009.1035
Version Text	AntiVir (7.9.1.35)
Date	Mon Oct 12 11:48:27 2009
Known Viruses	

Loaded Drivers

Version	Driver Name	Date	Known Viruses
7001.6098	ANTIVIR3.VDF	Mon Oct 12 11:57:12 2009	1788775

Virus Scan Server

Version	1.70
Version Text	Final Release of SAP Virus Scan Server, Copyright (c) SAP AG 1992-2009
Start Time	Mon Oct 12 14:14:04 2009
Production Data	Release 701, Level 0, Patch 29 for PC with Windows NT on Feb 4 2009 (mt.optunicode.SAP_CHAR/size_tvoid=16/32/32)

Adapter Data

Manufacturer	Avira GmbH
Product Name	AntiVir Virus Scan Adapter
Version	1001.3

One entry chosen

The following parameters are supported by Avira AntiVir for SAP:

Supported Parameters

Parameters	Type	Initial	Parameter Value
INITTEMP_PATH	CHAR	✓	E:\VSA\temp\ASV\$0E400000.TMP\
SCANBESTEFFORT	BOOL		1
SCANALLFILES	BOOL		1
SCANALLEMMBEDDED	BOOL		1
SCANHEURISTICLEVEL	INT		0
SCANEXTRACT	BOOL		1
SCANEXTRACT_SIZE	SIZE_T		1073741824
SCANEXTRACT_DEPTH	INT		5
SCANEXTRACT_RATIO	INT		150

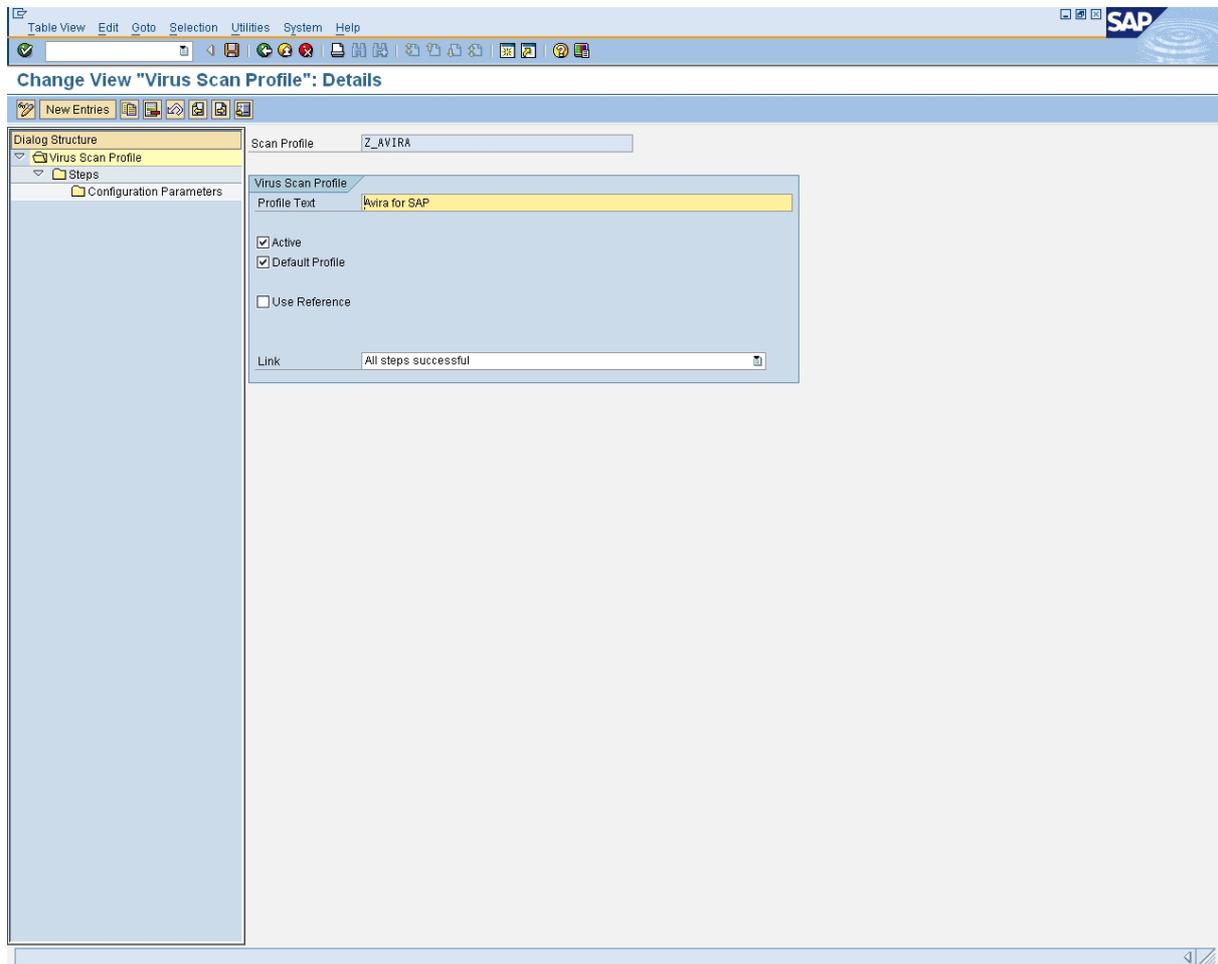


All parameters are activated by default except for the parameter SCANHEURISTICLEVEL. You can activate it in the menu 'vscanprofile' afterwards.

Definition for profiles which control the activation of the VSA

Transaction vscanprofile

Virus Scan Profile	Active	Default Prof.	Profile Text
/SARC/ARCHIVING_ADR	<input type="checkbox"/>	<input type="checkbox"/>	Virus Protection Using the Archive Developer
/SCET/GUI_UPLOAD	<input type="checkbox"/>	<input type="checkbox"/>	File Upload Using CL_GUI_FRONTEND_SER
/SCMS/KPRO_CREATE	<input type="checkbox"/>	<input type="checkbox"/>	
/SIHTTP/HTTP_UPLOAD	<input type="checkbox"/>	<input type="checkbox"/>	File Upload Using the Method CL_HTTP_ENTI
Z_ACTIVECONTENT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Active Content Scanning
Z_AVIRA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Avira for SAP



Scan Profile: Specifies the name of a virus scan profile.

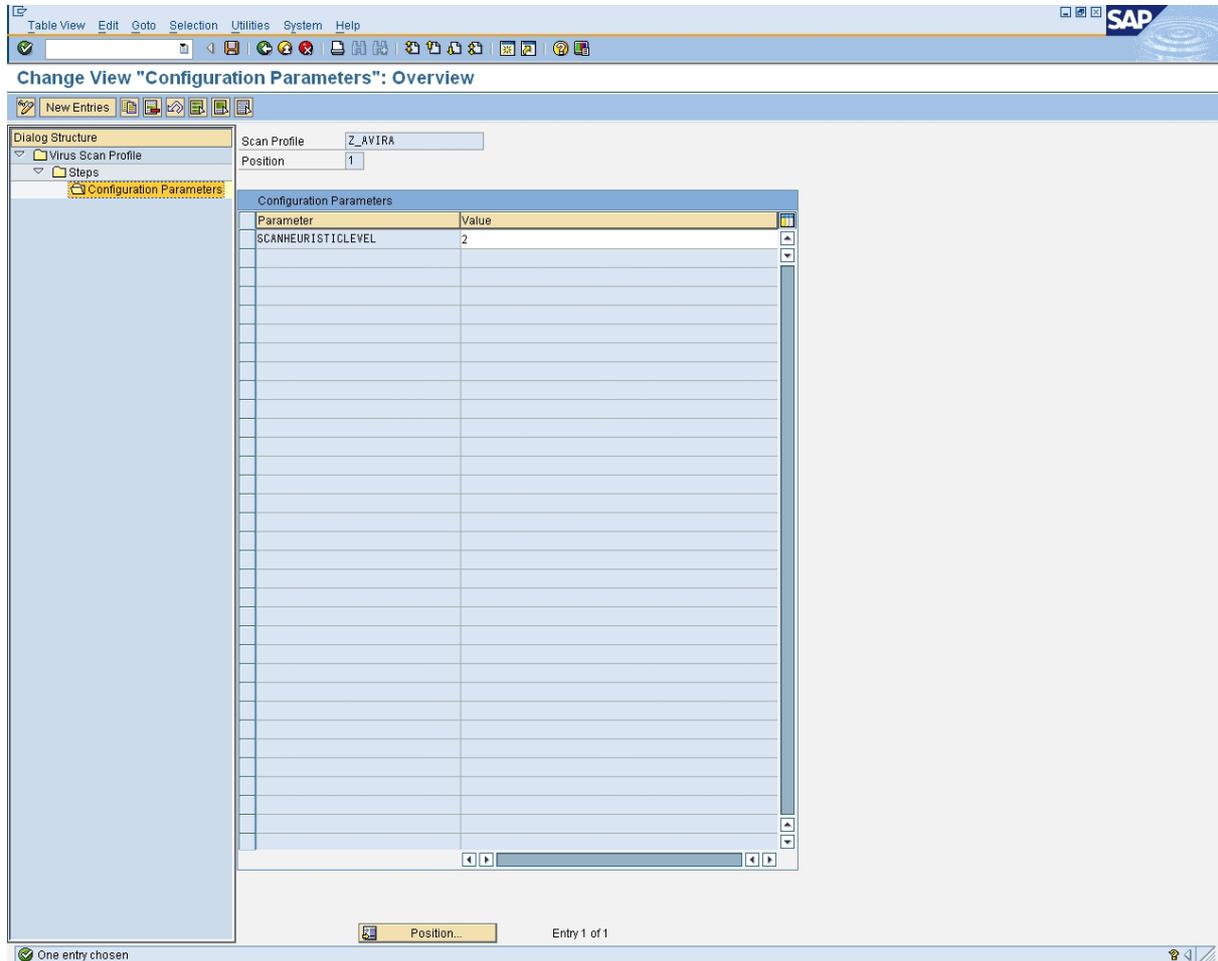
Profile Text: Explanatory text for a virus scan profile.

Active: Specifies that this virus scan profile is active. The virus scan profile can only be used if this indicator is set. SAP applications can use fixed profile names that are delivered. By default, these profiles are not active, meaning that the application program works without a virus scan. You can activate the virus scan for each application by setting this indicator.

Default Profile: Indicator that this virus scan profile is the default profile. You can set this indicator for only one virus scan profile. This virus scan profile is used in the following cases:

- If an application requests a virus scanner without specifying a virus scan profile.
- If a virus scan profile is requested for which the *Use Reference Profile* indicator is set, and the *Reference Profile* is empty.

Use reference: To operate multiple applications using the same virus scan profile, set the *Use Reference* indicator and specify the reference profile.



In case a virus scan profile uses several scanner groups, you can serialize them by a position number.

Type: Specifies whether a step in the virus scan profile refers to a scanner group or another virus scan profile. If you choose Group, the system uses a virus scan server from this group (or a BADI* implementation) for the virus scan. If you choose Profile, the program processes the specified virus scan profile instead of this step. You can define any conditions by combining the steps of the virus scan profile with the linkage type of the steps (AND/OR).

* The abbreviation BADI means business add-in. BADIs are the object related successors of user-exits. In comparison to the common [CMOD/SMOD](#)-extension they are more difficult to use. But they offer amplified development and modification possibilities. A BADI interface (transaction SE18) can contain different BADI implementations (transaction SE19) but only one can be active at the same time. You can realize interesting combinations of different BADIs. You can find all BADIs for each transaction by means of the following steps: 1. Transaction SE24 (Display class cl_exithandler); 2. Double-click on method GET_INSTANCE; 3. Enter breakpoint in line 25 (CASE sy-subrc); 4. Start transaction, execute the corresponding actions and wait for the debugger; 5. Evaluate the content of the box exit_name.



Scanner Group: Combines multiple virus scan servers or allows the use of a BAdI implementation. All of the virus scan servers of a scanner group have the same set of configuration parameters and will therefore use the same scan engine.

Viren Scan Profile: Specifies the name of a virus scan profile that you can include as a step in the profile that you are currently processing.

Testing the installation of the Virus Scan Server (Profile Z_AVIRA)

This procedure gives you the possibility to check your configured virus scan server.

- ▶ Start the transaction VSCANTEST.
- ▶ Enter the object you want to scan, the given test file or you own local file.

The screenshot shows the SAP 'Test for Virus Scan Interface' transaction. The window title is 'Test for Virus Scan Interface'. The interface is divided into three main sections: 'Object to Be Checked', 'Scanner Selection', and 'General Settings'. Under 'Object to Be Checked', 'Test Data' is selected with 'EICAR Anti-Virus Test File' in the dropdown. Under 'Scanner Selection', 'Virus Scan Profile' is selected with 'Z_AVIRA (Defaultprofil)' in the dropdown. Under 'General Settings', 'Display Scan Details' is checked, and 'Action' is set to 'Check Only'.

- ▶ Choose the virus scan profile, the scanner group or the virus scan server.
- ▶ Choose an action.



SAP

Result

✖ Return Value: 2- (At least one virus found)

Infections

ID	Virus Name	Object
39299	Eicar-Test-Signature	E:\usr\sap\NSP\tmp\26RSIVZ_AVIRA

Message List:

Typ	Message Text	LTxt
🟡	Start the processing of virus scan profile Z_AVIRA	
🟢	Virus scan profile Z_AVIRA, step 01: scanner group ANTIWIR	
🟢	Virus scan server VSCAN_AVIRA_WIN was selected from scanner group ANTIWIR	
🟢	Virus scan profile Z_AVIRA, step 01: scan instance returns 2- (At least one virus found)	
🔴	Virus "39299:Eicar-Test-Signature" found in object "E:\usr\sap\NSP\tmp\26RSIVZ_AVIRA"	🔍
🟢	Profile Z_AVIRA failed, since step 01 failed (AND linkage)	



Trace possibilities in the SAP system

- ▶ Transaction vscantrace
- ▶ Definition of a trace log for certain events

Program Edit Goto System Help

Virus Scan Server Trace

Virus Scan Server Control

Virus Scan Servers VSCAN_AVIRA_WIN OOO

Current Trace Level 0

Memory
File

Activate Deactivate Copy

Components for Trace Output

Visible Trace Level 11.262

- Server Errors
- Virus Infections
- Virus Scan Adapter Functions
- Virus Scan Adapter API Functions
- Server Warnings
- Server Information
- Parameter Operations in the Virus Scan Adapter
- RFC Functions of the Virus Scan Server
- RFC Parameters and/or Table Contents of Virus Scan Server
- Server Instances
- Server Memory

Trace Administration

- Self-Trace of the Memory Trace
- Record Everything



Trace possibilities in the SAP System

- ▶ Transaction vscantrace
- ▶ Trace runs and recollects data

Virus Scan Server Trace Output

Virus Scan Provider:	VSCAN_AVIRA_WIN
Availability of the Anti-Virus Engine	CC ●
Virus Scan Server Utilization	0
Trace Level	0

No Data Exists



Trace possibilities in the SAP System

- ▶ Transaction vscantrace
- ▶ Trace runs and collects data
- ▶ A file with an eicar (test virus) has been uploaded

```
List Edit Goto System Help
Virus Scan Server Trace Output
Update Delete Export Status Stop Configuration Test
Virus Scan Provider: VSCAN_AVIRA_WIN
Availability of the Anti-Virus Engine: CC
Virus Scan Server Utilization: 0
Trace Level: 11.262

2009-10-12T14:41:34.984 p002716 t3628 [vscan_rfc..VSCAN_RFC_LO:1933]: *RFC* >>> start >>> VSCAN_RFC_LOAD(1) >>> RfcAccepts=3, MODE=running
Sending data
  EF_LOAD (I): 0
  EF_NOT_AVAILABLE (C):
2009-10-12T14:41:34.984 p002716 t3644 [vscan_rfc..VSCAN_RFC_SC:2983]: *RFC* >>> start >>> VSCAN_RFC_SCAN_BYTES(3) >>> RfcAccepts=2, RfcBusy=1, MODE=running
Received data
  IF_DATA (X): RFC_XSTRING of length 68
  IF_JOB_ID (C): Z_AVIRA
  IF_WITH_DETAILS (C): X
  IF_WITH_ACFILTER (C):
Table content IT_SCAN_PARAM (1 lines):
-----
SCANHEURISTICLEVEL | INT | 2
-----
Table content ET_SCANERROR (0 lines):
Table content ET_INFECTIIONS (0 lines):
Table content ET_CONTENTINFO (0 lines):
2009-10-12T14:41:34.984 p002716 t3644 [vsixx.c :VsiGetInstan: 409]: *VSI* >>> start >>> VsiGetInstance(02112100)
2009-10-12T14:41:34.984 p002716 t3644 [vsixx.c :VsiGetInstan: 438]: *VSI* << end << VsiGetInstance(0219C3F0)
2009-10-12T14:41:34.984 p002716 t3644 [vscan_rfc..VSCAN_RFC_SC:2575]: * I * >>> start >>> VSCAN_RFC_SCAN(0,1,2_AVIRA,02E58F98,45937732,02BCF44C,021BCF68,021E1D58,0219DDA0)
2009-10-12T14:41:34.984 p002716 t3644 [vscan_rfc..VSCAN_RFC_SC:2590]: *VSI* scanning bytes with length 68
2009-10-12T14:41:34.984 p002716 t3644 [vsixx.c :VsiSetParame: 840]: *VSI* >>> start >>> VsiSetParameter(0219C3F0,SCANHEURISTICLEVEL,INT,2
2009-10-12T14:41:34.984 p002716 t3644 [vsixxi.c :VsiGetVsaFa:1103]: *PAR* Parameter SCANHEURISTICLEVEL is an optional parameter
2009-10-12T14:41:34.984 p002716 t3644 [vsixxi.c :VsiSetConfi:1462]: *PAR* Parameter SCANHEURISTICLEVEL was set with value 2
2009-10-12T14:41:34.984 p002716 t3644 [vsixx.c :VsiSetParame: 889]: *VSI* << end << VsiSetParameter(VSI_RC=VSI_OK)
2009-10-12T14:41:34.984 p002716 t3644 [vsixx.c :VsiScanClean:1784]: *VSI* >>> start >>> VsiScanClean(0219C3F0,ScanCode=2,ActionCode=2,00000000,Z_AVIRA,02E58F98,68,JobID=01,Infop
2009-10-12T14:41:34.984 p002716 t3644 [vsixx.c :VsiScanClean:1835]: * I * This VSA does not support scanning bytes - copy bytes to file and scan this
2009-10-12T14:41:34.984 p002716 t3644 [vsixxi.c :VsiFAlloc: 1537]: * M * memy alloc (ptr=021A8F38,size=25,clean=0)
2009-10-12T14:41:34.984 p002716 t3644 [vsixxi.c :VsiIXScan :2429]: *VSA* >>> VsaScan(02AC3C30,0219C4D8,0219C440,0219C500,00000000) >>
2009-10-12T14:41:34.984 p002716 t3644 [vsixxi.c :VsiIXScan :2446]: *VSA* << VsaScan(02AC3C30,0219C4D8,0219C440,0219C500,02AC4DF8) = -2 <<
2009-10-12T14:41:34.984 p002716 t3644 [vsixxi.c :VsiIXScan :2457]: *VIR* *** VIRUS alert! The object contains an infection.
2009-10-12T14:41:34.984 p002716 t3644 [vsixxi.c :VsiIXScan :2542]: * I * Scan report:JobID=0:Scanned=0::NotScanned=0:Clean=0:Infections=1:ScanErrors=0
2009-10-12T14:41:34.984 p002716 t3644 [vsixxi.c :VsiEXFree :1587]: * M * memy free (ptr=02111408)
2009-10-12T14:41:34.984 p002716 t3644 [vsixxi.c :VsiEXFree :1587]: * M * memy free (ptr=021A8F38)
2009-10-12T14:41:34.984 p002716 t3644 [vsixx.c :VsiScanClean:1907]: *VSI* << end << VsiScanClean(VSI_RC=VSI_E_VIRUS_FOUND)
2009-10-12T14:41:34.984 p002716 t3644 [vsixx.c :VsiEnumInfec:1959]: *VSI* >>> start >>> VsiEnumInfections(0219C3F0,0,...)
2009-10-12T14:41:34.984 p002716 t3644 [vsixx.c :VsiEnumInfec:2051]: *VSI* << end << VsiEnumInfections(VSI_RC=VSI_OK)
2009-10-12T14:41:34.984 p002716 t3644 [vscan_rfc..VSCAN_RFC_SC:2746]: * I * <<< end rc=0 <<< VSCAN_RFC_SCAN(0,1,2_AVIRA,02E58F98,68,-2,021BCF68,021E1D58,0219DDA0)
Sending data
  EF_SCANRC (I): -2
Table content IT_SCAN_PARAM (0 lines):
Table content ET_SCANERROR (0 lines):
Table content ET_INFECTIIONS (1 lines):
-----
89299 | Eicar-Test-Signature | E:\usr\sap\NSF\temp\SUXH232_AV.
-----
Table content ET_CONTENTINFO (0 lines):
2009-10-12T14:41:35.000 p002716 t3644 [vscan_rfc..VScanReturnI:1427]: *TRM* New thread 3644 was created. 6 (-ThAdM:1) threads active, 3 are waiting.
```



Activation of the Active Content Scanning

Transaction vscanprofile

How to enter a new virus scan profile ZACTIVCONTENT

The screenshot shows the SAP 'Virus Scan Profile: Overview' dialog box. The table below lists the profiles and their configurations:

Virus Scan Profile	Active	Default Prof.	Profile Text
/SARC/ARCHIVING_ADK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus Protection Using the Archive Developer
/SCET/GUI_UPLOAD	<input checked="" type="checkbox"/>	<input type="checkbox"/>	File Upload Using CL_GUI_FRONTEND_SER
/SCMS/KPRO_CREATE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
/SIHTTP/HTTP_UPLOAD	<input checked="" type="checkbox"/>	<input type="checkbox"/>	File Upload Using the Method CL_HTTP_ENTI
ZACTIVCONTENT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Active Content Scanning
Z_AVIRA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Avira for SAP

Beneath *Steps*, the virus scan profile ZACTIVCONTENT has to be assigned to a group. Therefore a new group can be defined or an already existing group can be used.



Testing the Installation of the Virus Scan Server (profile ZACTIVECONTENT)

This procedure allows you to check the function of the virus scan server you have configured.

- ▶ Start the transaction VSCANTEST
- ▶ Enter the object you want to check. You can use the given test files or you own local file

The screenshot shows the 'Test for Virus Scan Interface' dialog box in SAP. The window title is 'Test for Virus Scan Interface' and it features the SAP logo in the top right corner. The interface is divided into three sections: 'Object to Be Checked', 'Scanner Selection', and 'General Settings'. In the 'Object to Be Checked' section, the 'Local File' radio button is selected, and the text 'C:\temp\test.html' is entered in the adjacent text field. In the 'Scanner Selection' section, the 'Virus Scan Profile' radio button is selected, and 'ZACTIVECONTENT (Defaultprofil)' is entered in the text field. In the 'General Settings' section, the 'Display Scan Details' checkbox is checked, and 'Check for Active Content' is selected in the 'Action' dropdown menu.

Choose the scan profile you want to use for the scan beneath virus scan profile. This example uses the profile ZACTIVECONTENT.

In the *General Settings* you choose the action “Scan for active content”.



Result

✖ Return Value: 3- (At least one macro was found)

Infections

ID	Virus Name	Object
	active content	E:\usr\sap\NSP\tmp\RVPRPrtest.html

Message Text

Ty.	Message Text	LTxt
■	Start the processing of virus scan profile ZACTIVECONTENT	
■	Virus scan profile ZACTIVECONTENT, step 01: scanner group ANTVIR	
■	Virus scan server VSCAN_AVIRA_WIN was selected from scanner group ANTVIR	
■	Virus scan profile ZACTIVECONTENT, step 01: scan instance returns 3- (At least one macro was found)	
✖	Virus "active content" found in object"E:\usr\sap\NSP\tmp\RVPRPrtest.html"	
■	Profile ZACTIVECONTENT failed, since step 01 failed (AND linkage)	

Integration of the VSA without RFC destination

- ▶ It is possible to load the virus scanner directly into the SAP Netweaver
- ▶ Choose virus scan adapter in the transaction "vscan" provider type
- ▶ **Important:**
The basic system has to be supported by Avira if you want to use the provider type "virus scan adapter".



Environment variables VSA_LIB and VSA_DEBUG

- ▶ Used environment variables (Windows)
- ▶ VSA_LIB: refers to the antivirvsa.dll
- ▶ The variable is entered automatically
- ▶ VSA_DEBUG: refers to a path of the debug log file of the VSA
- ▶ Variable value, f.ex. „C:\avsapvsa.log“

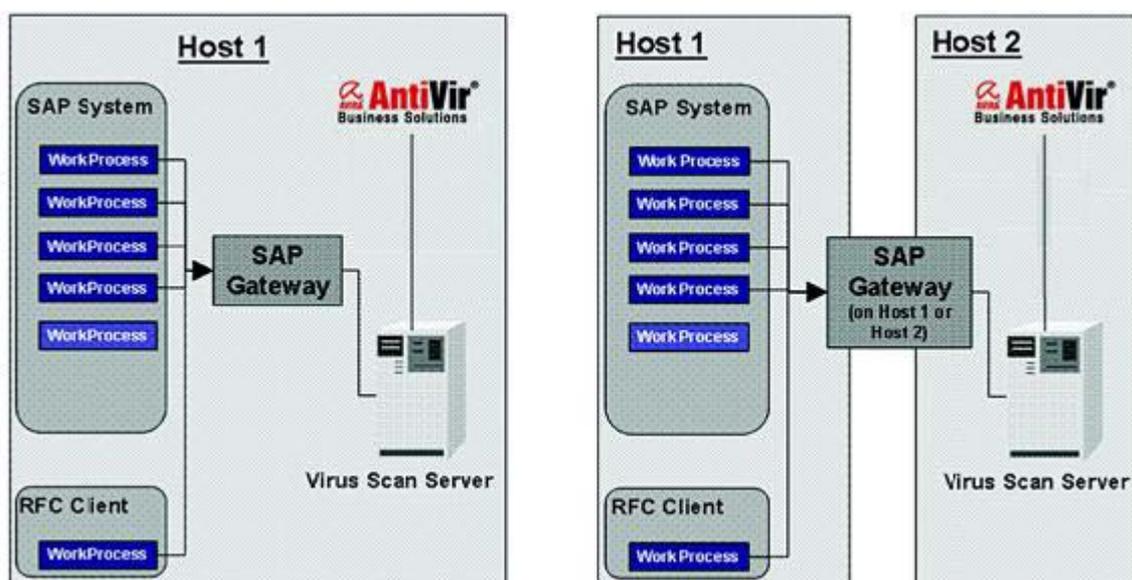
Application server or self-starter

You can install an application server starter (started by the application server) or a self-starter (f. ex. externally as service with Microsoft Windows NT or daemon beneath UNIX) for the configuration of a virus scan server for ABAP systems.

In case the application server starter is used, all components are located on the same host.

In case of the self-starter, the virus scan server and the SAP WebAS can be located on different hosts. So you can use a virus scan server which is available only for a certain platform, even though the SAP Web AS is installed on a different platform!

Here you see the virus scan server on one or on two hosts:





In the running system the difference between application starter and self-starter affects the Computing Center Management System (CCMS). You can supervise the virus scanners by means of the CCMS (transaction RZ20) in the “SAP CCMS Monitors for Optional Components” in the monitor Virus Scan Server (you find further information on the SAP website)

The following differences have to be taken into consideration:

• **Application server starter:**

The file collector of the CCMS checks automatically if a configured virus scan server is reachable. In case there is no virus scan server available the CCMS triggers an alert and starts the virus scan server again as an auto reaction.

• **Self-starter:**

However there is a separate MTE class in CCMS for these self-starters. You can assign an auto-reaction method to this MTE class yourself to react to alerts. You can, for example, use the MTE class CCMS_OnAlert_Email to send an e-mail or an SMS (see "Defining Automatic Alert Notification" and "Forwarding Alerts to Alert Management (ALM)" on the SAP website).

External activation of the AntiVir VSA via VSCAN_RFC (self-starter)

Command line windows:

▶ `vscan_rfc -a VSCAN_Localhost -g vmserv1 -x 3300 -V „c:\vsa\antivirvsa.dll“`

Command line Linux:

▶ `vscan_rfc -a VSCAN_Localhost -g vmserv1 -x 3300 -V „/usr/lib/Antivir/libantivirvsa.so“`

Description of the parameters:

-a Programm ID (RFC Destination)
-g Gatewayhost
-x Port vom SAP Gateway
-V Pfad zur lokalen Lib



Scan of SAR and CAR archives

Usually the Avira Virus Scan Adapter is unable to unpack such archives. But you can influence this behavior by means of the configuration file savapi.ini which you find in the installation directory.

The screenshot shows three windows. The left window is Notepad with the following configuration for savapi.ini:

```
[SAVAPI2SERVICE]
SapCarProgram=E:\usr\sap\NSP\SYS\exe\uc\NTI386\sapcar.exe
PortNumber=18370
TempDirectory=C:\Program Files\Avira\VSA\temp\
UpdatedDirectory=C:\Program Files\Avira\VSA\update\
KeyFileName=C:\Program Files\Avira\VSA\hbedv.key
LogFileName=C:\Program Files\Avira\VSA\savapi.log
LogFileSize=1000
ReportLevel=0
AttachToGuard=1
UpdateUrl=http://d1.antivir.de
UpdateInterval=120
NetworkUserName=
NetworkPassword=
ProxyEnabled=0
ProxyPort=
ProxyUrl=
ProxyUserName=
ProxyPassword=
SmtMailEnabled=0
SmtMailMode=0
SmtHostName=
SmtSenderAddress=
SmtRecipientAddress=
```

The middle window shows the File Explorer for E:\VSA, listing files and folders such as backup, temp, update, antivir0.vdf, antivir1.vdf, antivir2.vdf, antivir3.vdf, antivirvsa.dll, avewin32.dll, avpack32.dll, dwwld.dll, DwwldSvc.exe, hbedv.key, lic_info.txt, msvcr71.dll, msvcrt.dll, readme.htm, savapi2m.dll, savapi2r.dll, savapi2s.exe, savapi.dll, savapi.ini, savapi.log, smtplib.dll, StartUpdate.exe, and unacev2.dll.

The right window shows the File Explorer for E:\usr\sap\NSP\SYS\exe\uc\NTI386, listing files such as ntreg2cmd.exe, R3ntreg2env.exe, ntsmgr.exe, R3ldctl.exe, R3load.exe, R3loadada.pdb, R3szchk.exe, R3ta.exe, R3ta.pdb, R3trans.exe, R3trans.pdb, rfcexec.exe, rfcexec.sec, rseparulib.dll, rscpf2f.exe, rscpf3f.exe, rscpf_ars.exe, rscpf_db.exe, rspoconnector.dll, rstrscs.exe, rstrfile.exe, rstrlscs.exe, rstrscs.exe, rsyn.bin, sapcar.exe, and sapccm4x.exe.

Hints:

This adjustment of the Avira Virus Scan Adapter is possible with both, a windows ABAP system and a windows Java system.

In Unix you find the configuration file „avsapvsa.conf“ in the directory /etc/.

In this file a link to the SAPCAR program via the parameter „SapCarProgram“ is possible.