How-to Guide
SAP NetWeaver ‘04

How To… configure the Virus Scan Service for KM

Version 1.00 – September 2006

Applicable Releases:
SAP NetWeaver ’04 SPS 9

1 Scenario

You use the Knowledge Management capabilities of SAP NetWeaver to work with documents. You might already use virus scan technology at your company for security reasons. Nowthat users can access Knowledge Management from outside your company network through the portal, you also want to integrate virus scan technology in Knowledge Management.

2 Introduction

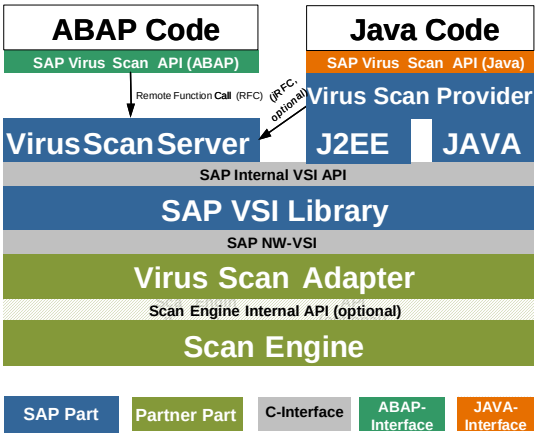
Due to the increasing number of malware you are looking for means to protect your systems against viruses, worms, and so on. Typically, company-wide use of virus scanners at file system level is standard. Now, companies are also interested in extending protection to Knowledge Management.

SAP does not provide a specific solution for virus scanning, but delivers an API that partners can use to integrate their virus scan solution in SAP NetWeaver.

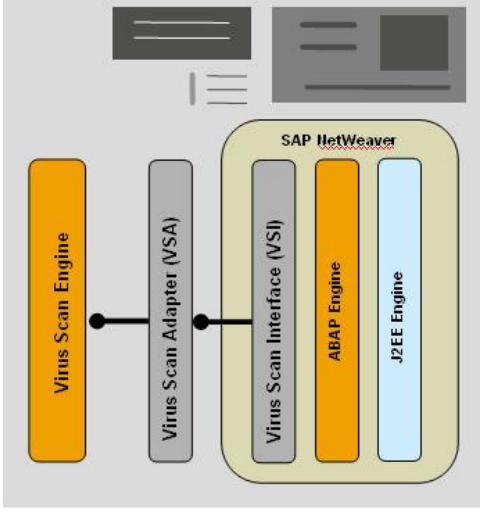
As of SAP NetWeaver ’04 SPS 9, you can integrate an external virus scanner in Knowledge Management for checking documents when they are accessed. This check also ensures that no infected documents are distributed in Knowledge Management.

3 Architectural Overview

The adjacent figure shows the main components of the virus scan integration concept. In this figure, the different colors differentiate the components relating to the programming language and the provider. The virus scan interface (VSI) provides an interface for ABAP and JAVA. Depending on the programming language, the VSI library communicates with the virus scan server or the virus scan provider. The virus scan adapter (VSA), which is implemented by partners, communicates with the VSI library. This means that the partner only needs to provide a single VSA implementation for both ABAP and JAVA.



Basically, you can install the virus scan engine and SAP NetWeaver on a single-server system. The adjacent figure shows the components and the communication path in this scenario. The advantage of this configuration is the faster communication compared to remote function calls (RFC), due to the usage of native communication based on shared libraries. However, the load originating from the virus scan engine can significantly affect the performance of SAP



NetWeaver because the same hardware resources are used.

It is also possible to separate the virus scan engine and the SAP NetWeaver installation to avoid impacting performance due to shared hardware resources. The disadvantages are slower communication and higher network traffic volume because all scanned documents need to be transferred from SAP NetWeaver to the virus scan engine.

For a better understanding of the configuration explained in detail later on, you must know what the terms virus scan group and virus scan provider mean.

A *virus scan group* combines one or more virus scan engines, which are represented by virus scan providers. These are all to be used in the same way to check documents. If more engines are used, the check requests are sent to one engine after an other to distribute the load between the engines (round robin method).

A *virus scan provider* represents the interface to the virus scan engine in the flavors virus scan adapter and virus scan server. A virus scan adapter is used for VSI library-based communication as explained above, whereas a virus scan server is used when the virus scan engine and SAP NetWeaver are installed on separate server systems.

Based on an example, the following sections describe the steps for the configuration on the Java application server and in Knowledge Management. In addition, several screenshots illustrate the main use cases. At the end of this guide, there are links to more information.

4 Prerequisites

Before starting the configuration, you must prepare an adequate portal landscape. We strongly recommend starting the configuration on a test landscape and not on a production landscape to avoid downtime of the production system. In addition, you must check in SAP Note 782963 which external virus scan solutions are currently supported and install them correctly.

The following section describes the configuration of an example implementation of the virus scan adapter. This example implementation does not offer a scan function because it in fact does not use a virus scan engine as a real virus scan adapter would do. However, the configuration does not differ from a virus scan adapter from a partner and could therefore be used even if no virus scan engine is yet available.

The example implementation is attached to SAP Note 786179, which is aimed at partners who want to integrate their virus scan solution in SAP NetWeaver. The example implementation uses a simple use case to explain the coding.

5 The Step By Step Solution

The following description focuses on the configuration of a JAVA application server and of KMC. For the usage of the virus scan interface in ABAP applications, it refers to the standard documentation on the SAP Help Portal at http://help.sap.com.

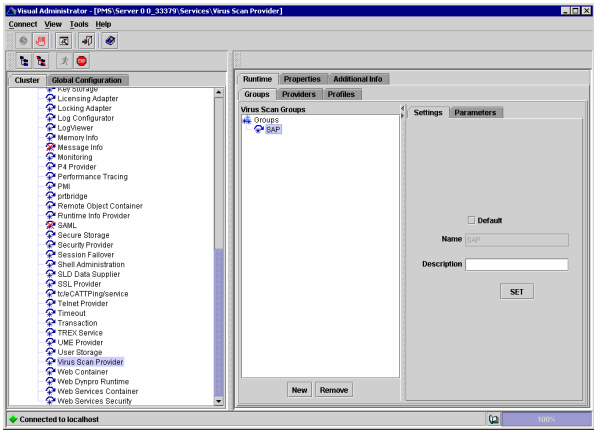
We can separate the entire configuration of the virus scan integration into two parts. The first part consists of configuration steps on the JAVA application server. Based on this configuration, the second part focuses on configuration steps on the KMC configuration UI.

The next section starts with the configuration steps on the JAVA application server.

5.1 Configuration of the JAVA Application Server

1. Configure a virus scan group

Start the Visual Administrator for your JAVA application server and open the virus scan provider



service. Navigate to *Runtime* → *Groups* and choose *New*. Enter *SAP* in the *Name* field and any text in the *Description* (optional).

The screenshot shows the Visual Administrator and the corresponding group definition.

2. Configure a virus scan adapter

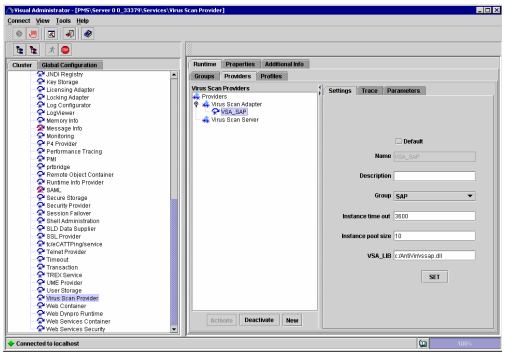
Navigate to the *Runtime* → *Providers* tab and select the *Virus Scan Adapter* entry. Choose *New* to create a new entry. Enter a meaningful name. In this example, we have chosen *SAP*. Keep in mind that the the name is case-sensitive and that the systems add the prefix *VSA_* to your chosen name.

For example, if you enter SAP, the system creates *VSA_SAP*. Later on, in the Knowledge Management configuration, you will need to refer to this name.

In addition, you must define the *Group* and *VSA_LIB*

parameters. In this example, choose the previous group, SAP, as the group and enter the file system path to the example implementation of a virus scan adapter. Section 4 explains more details and where to get the implementation.

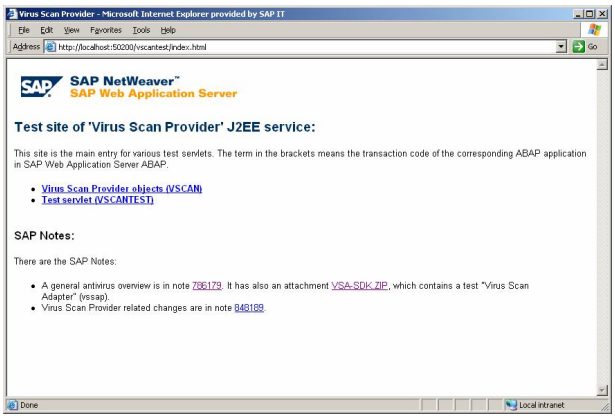
The screenshot shows the screen after entering all necessary parameters.



3. Test the configuration

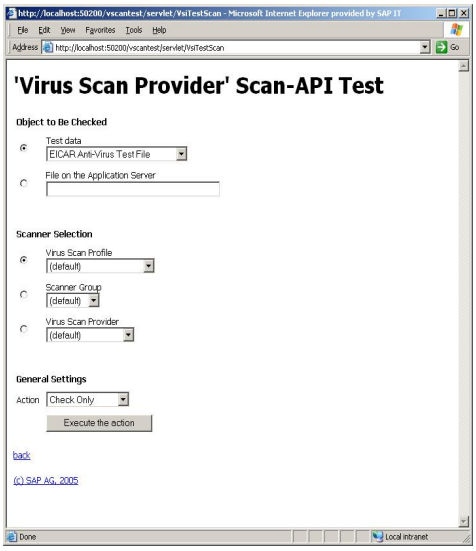
You have now completed all configuration settings in the Java application server. SAP provides a servlet that you can use to test the configuration.

Open a Web browser and enter `http://<server>:<port>/vscantest` to start the servlet.

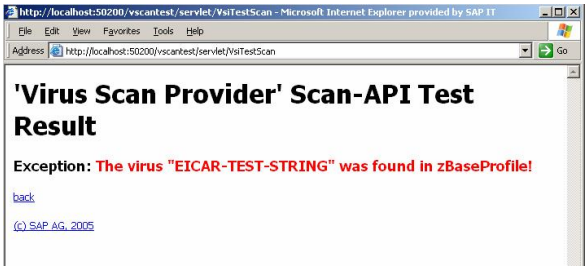


The screenshot above appears. Among the information it contains are links to more SAP Notes. The first link, *Virus Scan Provider objects (VSCAN)* provides an overview of the configuration.

The second link, *Test servlet (VSCANTEST)*, provides a form that you can use to specify the configuration test in more detail.



For example, select the *EICAR-Anti-Virus TestFile* as the *Object to be Checked*. Furthermore, select a group as the *Scanner Group*, in this example, SAP. Choosen *Execute* to start the test.



An exception appears, indicating that the test has found a valid virus signature. Keep in mind that the EICAR viurs signature is not an harmful virus. For more information about this test virus, see the appendix of this guide.

5.2 Configuration of Knowledge Management

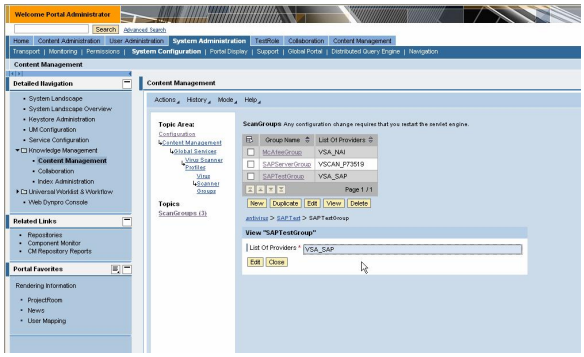
The second part of the configuration is done in the configuration framework of Knowledge Management using the configuration UI.

Note: Activate the advanced mode on the configuration UI, otherwise the virus scan-related entries are not displayed.

1. Configuration of a virus scan group

With the current release of Knowledge Management, you still have to configure virus scan groups and providers. This may change in future releases because the configuration is already available in the JAVA application server.

Navigate to *System Administration* → *System Configuration* → *Knowledge Management* → *Content Management* → *Global Services* → *Virus Scanner Profiles* → *Virus Scanner Groups*. Choose *New* to create a new virus scan group. In this example, just reuse the existing configuration, *SAPTestGroup*. Change the *List of Providers* to *VSA_SAP* parameter to reflect the case- sensitivity because the name is in uppercase letters io the JAVA application server.



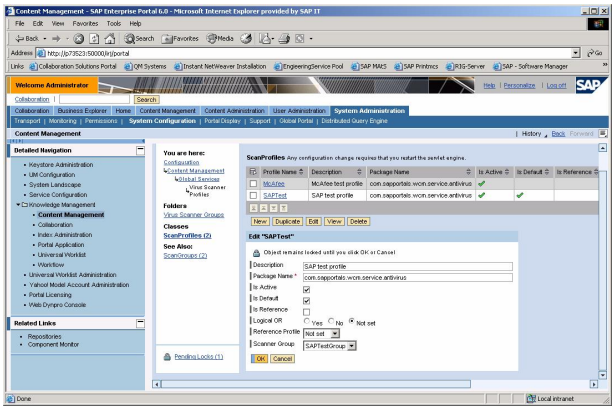
The screenshot above shows the example group definition.

2. Configuration of a virus scan profile

The next step is to configure a virus scan profile. Navigate to *System Administration* → *System Configuration* → *Knowledge Management* → *Content Management* → *Global Services* → *Virus Scanner Profiles*. Choose *New* to create a new entry. In this example, reuse the existing configuration, *SAPTest*. Open this configuration in edit mode and verify the following:

- The configurable is active
- The default checkbox is selected, as long as no other configurable is the default
- No reference profile is selected
- The previously-configured virus scan group,

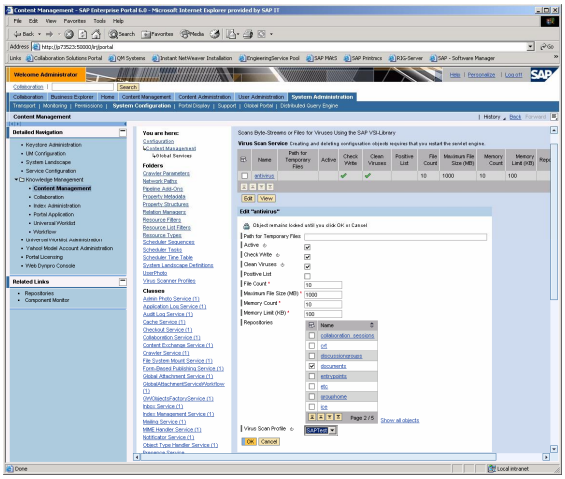
SAPTestGroup, is selected



The screenshot above illustrates the configuration. For more information about the configuration parameters, consult the online help at http://help.sap.com.

3. Configuration of the virus scan service

Finally, you have to configure the virus scan service for Knowledge Management. This configuration is probably the most important one because this is the location where you define the basic behavior of the virus check in Knowledge Management. The screenshot below shows the configuration screen.



First of all, you must make sure that the service is active. Check that the checkbox for the *Active* parameter is selected.

In this example, a virus check should be done when documents are written in Knowledge Management. Therefore, you must select the *Check Write* checkbox.

The combination of the *Positive List* and *Repositories* parameters defines which repositories are taken into account during checking. If the *Positive List* parameter is selected, the virus check is done in all repositories defined in the *Repositories* parameter. If it is not set, the system excludes all repositories defined in the *Repositories* parameter from the virus checks. In this example, every repository is checked

except the documents repository.

Note: You could use any repository in this example. A specific CM repository in DB mode is recommended instead of the standard documents repository for test purposes to avoid confusing side-effects with other use cases.

Finally, configure the reference to the virus scan profile. In this example, you choose the previous profile, *SAPTest*.

4. Restart the portal

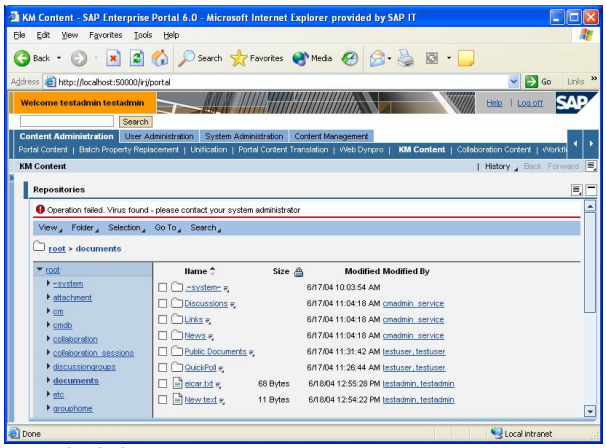
To activate the Knowledge Management configuration settings, you must restart the portal and the JAVA application server(s) that provides the portal functions.

5.3 Use Cases for Virus Scan Integration

This section describes the different use cases where virus scan integration in Knowledge Management is visible to the user. Basically, there are edit and read scenarios because they represent the main types of access to documents.

1. Access through browsers

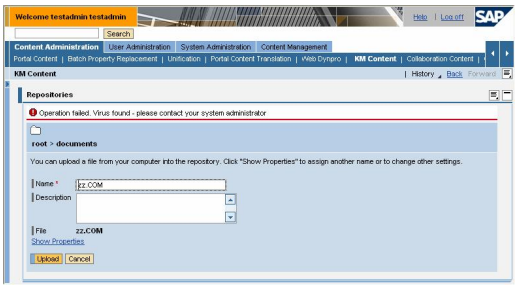
When a user accesses an virus-infected file, if the virus scan service is configured to check on read access, the following error message appears: *Operation failed: Virus found – please contact your system administrator*



Note: If the virus scan service is configured for checks on write access, *no* alert would appear!

The screenshot above shows the results.

When a user tries to upload an infected file, if the virus scan service is configured to check on write access, an alert would appear.

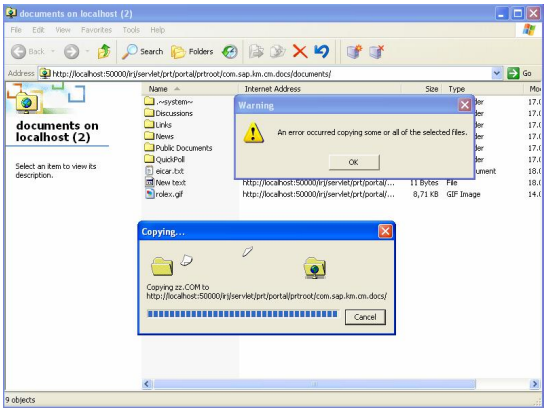


As in the case of a read access, the following error message appears:
Operation failed: Virus found – please contact your system administrator

Note: If the virus scan service is configured to check on read access, *no* alert would appear!

2. Access through WebDAV clients

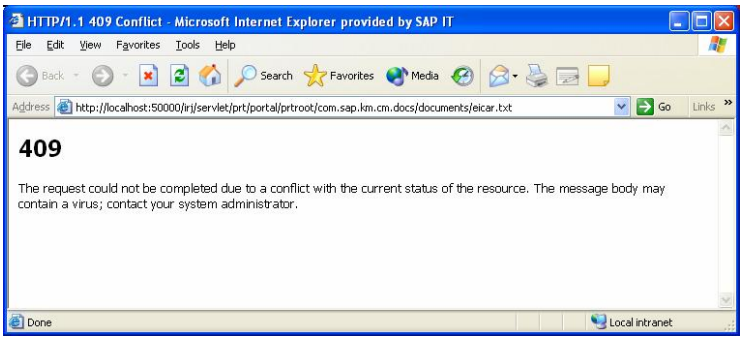
Authors and editors often use WebDAV clients to access documents in Knowledge Management. If an author tries to write an infected file to a Knowledge Management repository, an error message appears depending on the WebDAV client.



The screenshot above illustrates the behavior of Microsoft Internet Explorer.

Note: If the virus scan service is configured to check on read access, *no* alert would appear!

Reading a virus-infected file if the virus scan service is configured to check on read access would result in the http error 409 as shown in the screenshot below.



Note: If the virus scan service is configured to check on write access, *no* alert would appear!

6 Appendix

Additionally, Knowledge Management offers a specific virus scan report that allows you to check documents in a repository independent of read or write accesses. For example, this report could be used when integrating a file system with documents that are potentially infected. In this most common scenario for the report, you would configure the scanner service to check on write access. Then, the service would check any new documents created through Knowledge Management.

Since the previously executed report ensures that there are no infected files in the repository, there would be no further need to check for viruses on read access. However, if documents are stored directly on the file system without using Knowledge Management, suspicious files might be also accessible through Knowledge Management without further checks. In this case, you would have to schedule additional runs of the report or, even better, restrict direct file system access.

For more information about this report, see the SAP help portal at http://help.sap.com/saphelp_nw04/helpdata/en/b8/f5af401efd8f2ae10000000a155106/frameset.htm.

SAP also provides the WebDAV client, **Portal Drive**. For more information about this tool, see the SAP help portal at http://help.sap.com/saphelp_nw04/helpdata/en/42/c99b91341a6bade10000000a1553f6/frameset.htm. In addition, SAP Note **911449**, as the central note for the Portal Drive, provides information about the download path, among other things.

The test virus signature previously mentioned is provided by the European Institute for Computer Antivirus Research (**EICAR**) on http://www.eicar.org. This test file does not hurt anything but the virus scanner recognizes it as a virus and therefore you can use it as an easy test for virus scanner configuration in general.

For more information about the virus scanner interface provided by SAP or the availability of certified virus scanners, see the following notes:

- Note **782963**: Availability of virus scan server for NW-VSI
- Note **786179**: Data security products: Application in the antivirus area
- Note **666568**: Using the EICAR anti-virus test file

7 Change Log

Date	Release	Description
09/2006	1.00	First release

http://www.sdn.sap.com/irj/sdn/howtoguides