TREND MICRO™

9.6 Deep Security

Integration Guide for SAP

Advanced Protection for Physical, Virtual, and Cloud Servers

Cloud & Data Center

Complete End User

Cyber Threats

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Document version: 1.0
Release date: July 2015
Document generated: Nov 18, 2015 (10:14:26)

Introduction

Trend Micro Deep Security supports integration with the SAP NetWeaver platform.

The Trend Micro Deep Security Agent can be called by a library that is automatically deployed on SUSE Linux Enterprise Server 11 (SLES) 64-bit or Red Hat Enterprise Linux 6 (RHEL) 64-bit operating systems. This is available starting with Deep Security 9.5 build 2774 or later. It is officially supported in Deep Security Agent version 9.6.

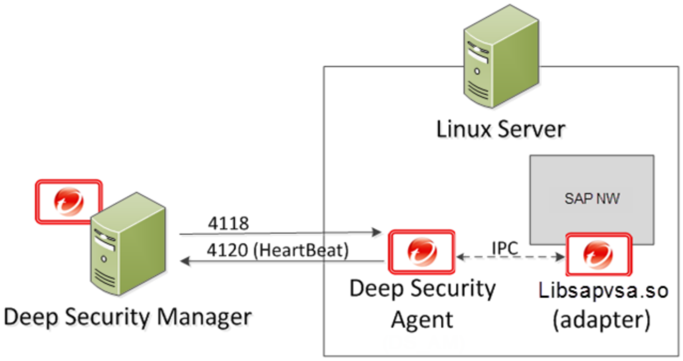
This is an overview of the integration steps:

1. Install the Deep Security Agent on an SLES 11- or RHEL 6-based SAP application server. See ***Install the Deep Security Agent (page 5)***.
2. Add the SAP server to Deep Security Manager and activate the Agent on the SAP server. See ***Adding the SAP Server to Deep Security Manager (page 6)***.
3. Apply a security profile that has Anti-Malware active to provide the Agent with the latest pattern and scan engine. See ***Assign a Security Profile (page 9)***.
4. Configure the SAP Virus Scan Interface (VSI) by calling the following transactions. See ***Configure SAP to Use the Deep Security Agent (page 12)***:
    - VSCANGROUP
    - VSCAN
    - VSCANPROFILE
    - VSCANTEST

Note: *Depending on your operating system and environment, the output that you see may differ slightly from what is shown in this guide.*

You can find other Deep Security documentation at http://docs.trendmicro.com/en-us/enterprise/deep-security.aspx. In addition, Deep Security Manager includes a help system that is available from within the Deep Security Manager console.

Deep Security and SAP Components



Deep Security Manager connects with the Deep Security Agent located on the SAP NetWeaver Linux server. The Agent connects with libsapvsa.so, which is the virus adapter provided by Trend Micro for scanning purposes.

The components involved in this solution are:

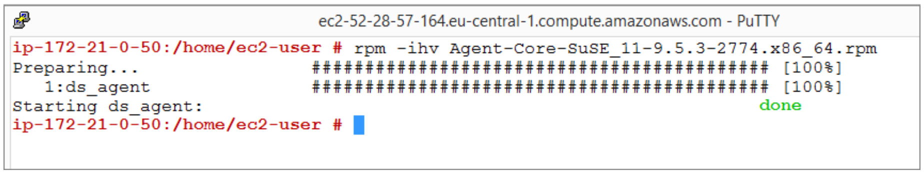
- **Deep Security Manager:** The centralized Web-based management console that administrators use to configure security policy and deploy protection to the enforcement components: the Deep Security Agent and the Deep Security Agent.
- **Deep Security Agent:** A security agent deployed directly on a computer. The nature of that protection depends on the rules and security settings that each Deep Security Agent receives from the Deep Security Manager.
- **SAP NetWeaver:** SAP integrated technology computing platform. The SAP NetWeaver Virus Scan Interface (NW-VSI) provides virus scanning capabilities for third-party products that perform the actual scan. The NW-VSI interface must be activated.
- **SAP NetWeaver ABAP WinGUI:** A Windows management console used for SAP NetWeaver. In this document, it is used for the configuration of the Deep Security Agent and the SAP NetWeaver Virus Scan Interface.

Install the Deep Security Agent

The Deep Security Agent is installed with core Agent functionality only. After the Agent is installed, you can enable Protection Modules on the Agent. At that point, the plug-ins required for the Protection Modules will be downloaded and installed.

To install the Deep Security Agent on SUSE Linux Enterprise Server or Red Hat Enterprise Linux:

1. Go to the Trend Micro Download Center (http://downloadcenter.trendmicro.com) and download the Deep Security Agent package for your OS.
2. Install the Agent on the target system. You can use **rpm** or **zypper**, depending on the OS. In this example, rpm is used by typing: `rpm -ihv Agent-Core-SuSE_11-9.5.3-2774.x86_64.rpm`
3. You should see output similar to what's shown in this example, which indicates that the Agent installation is complete:



```
ip-172-21-0-50:/home/ec2-user # rpm -ihv Agent-Core-SuSE_11-9.5.3-2774.x86_64.rpm
Preparing...                ########################################### [100%]
   1:ds_agent               ########################################### [100%]
Starting ds_agent:                                                     done
ip-172-21-0-50:/home/ec2-user #
```

Note: *You can also deploy the Agent using a deployment script generated from the Deep Security Manager.*

Adding the SAP Server to Deep Security Manager

The Agent is now installed on the SAP server but no protection modules are active. To enable protection, you need to add the SAP Server to the Deep Security Manager console.

Activate SAP in the Deep Security Manager

To enable the SAP features in the Deep Security Manager, you must enter an activation code:

1. In the Deep Security Manager, go to **Administration** > **Licenses**.
2. Click **Enter New Activation Code**.
3. In the **SAP Integration** area (under **Additional Features**), enter your SAP activation code, the click **Next** and follow the prompts.

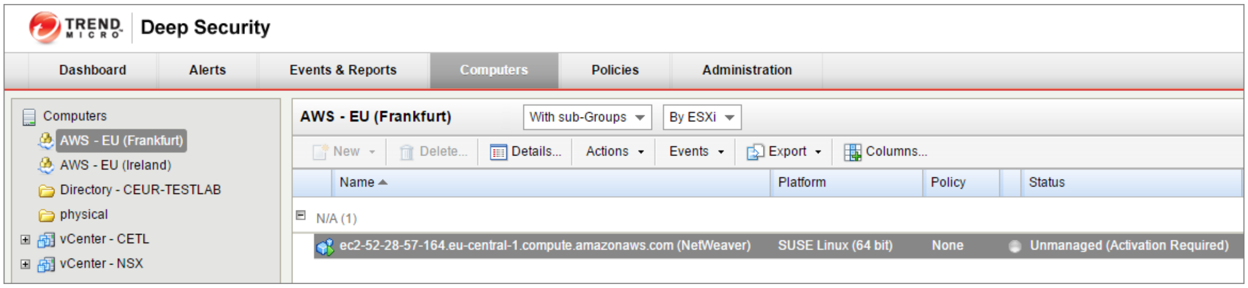
Note: *In order to use the SAP integration feature, the Anti-Malware and Web Reputation modules must also be activated.*

The **SAP** tab will now be available in the Computer/Policy editor, where you can enable the SAP integration feature for individual computers or policies.

Add the SAP Server

To add the SAP Server, open the Deep Security Manager console and on the **Computers** tab, click **New**. The are several ways to add the server, including synchronization with Microsoft Active Directory, VMware vCenter, Amazon Web Services, or Microsoft Azure. You can also add the computer using an FQDN or IP address. For detailed instructions, see the **Deep Security Manager Help**, which is available from Deep Security Manager console.

In this example, we have synchronized with an Amazon Web Service Account and see our instance, `ec2-52-28-57-164.eu-central-1.compute.amazonaws.com (NetWeaver)`:



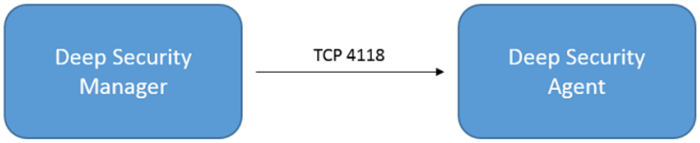
Name	Platform	Policy	Status
N/A (1)			
ec2-52-28-57-164.eu-central-1.compute.amazonaws.com (NetWeaver)	SUSE Linux (64 bit)	None	Unmanaged (Activation Required)

Activate the Agent

The status of your instance will be either **Unmanaged (Activation Required)** or **Unmanged (Unknown)**. Next, you will need to activate the Agent before the Manager can assign Rules and Policies to protect the computer. The activation process includes the exchange of unique fingerprints between the Agent and the Manager. This ensure that only one Deep Security Manager can communicate with the Agent. There are two ways to activate the Agent: **Agent-initiated** or **Manager-initiated**.

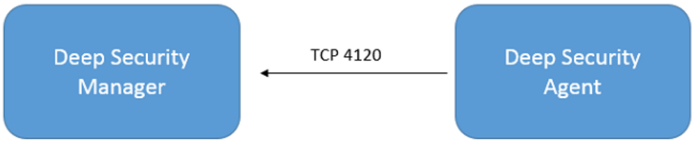
Manager-Initiated Activation

The **Manager-initiated** method requires that the Deep Security Manager can access the FQDN or the IP of the instance via TCP port **4118**. This can sometimes be difficult due to NAT-environments. To perform Manager-initiated activation, go to the **Computers** tab in the Deep Security Manager console, right-click the instance where the Agent is installed and click **Actions** > **Activate**.

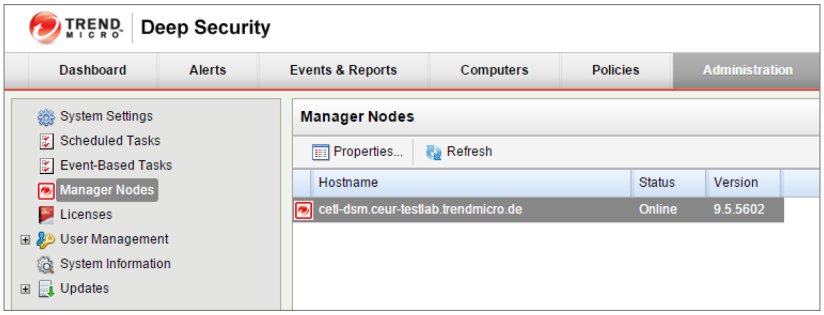


Agent-Initiated Activation

The **Agent-initiated** method requires that the Deep Security Agent can access the configured Deep Security Manager address via TCP port **4120**.



The configuration of the Deep Security Manager address (FQDN or IP) can be found in the Deep Security Manager console:



Manager Nodes

Hostname	Status	Version
cetl-dsm.ceur-testlab.trendmicro.de	Online	9.5.5602

You will also need to enable Agent-initiated activation from the Deep Security Manager console, by clicking **Administration** > **System Settings** > **Agents** and selecting **Allow Agent-Initiated Activation**.

Next, use a locally-run command-line tool on the Deep Security Agent to initiate the activation process. The minimum activation instruction contains the activation command and the Manager's URL (including the port number):

```
dsa_control -a dsm://[managerurl]:[port]/
```

where:

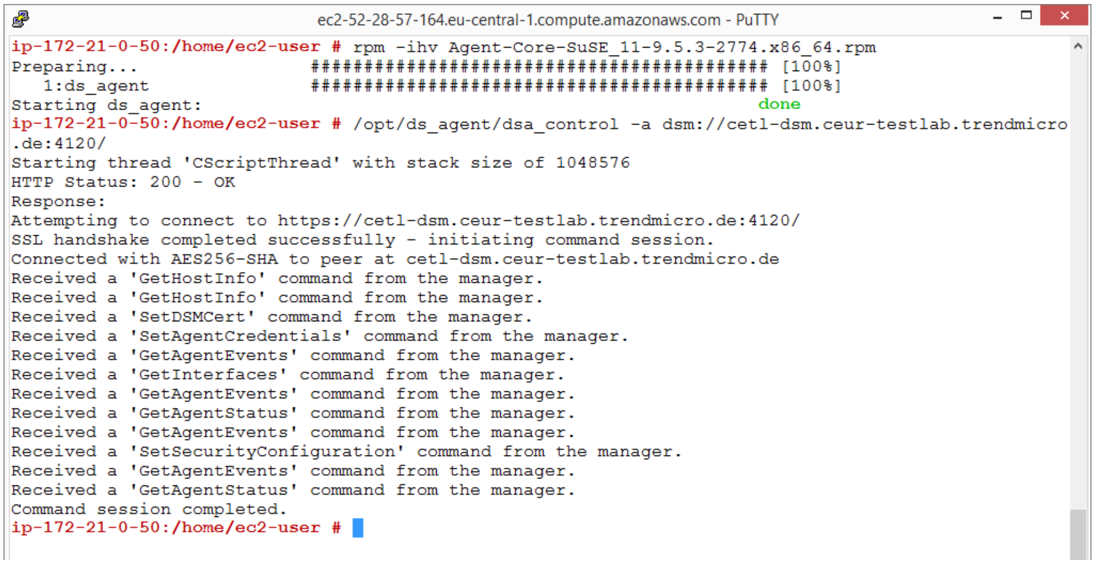
- **-a** is the command to activate the Agent , and

- **dsm://managerurl:4120/** is the parameter that points the Agent to the Deep Security Manager. ("managerurl" is the URL of the Deep Security Manager, and "4120" is the default Agent-to-Manager communication port.)

The Manager URL is the only required parameter for the activation command. Additional parameters are also available. (For a list of available parameters, see "Command-Line Utilities" in the Deep Security Manager Help.)

In the following example, we use the Agent-initiated activation by typing:

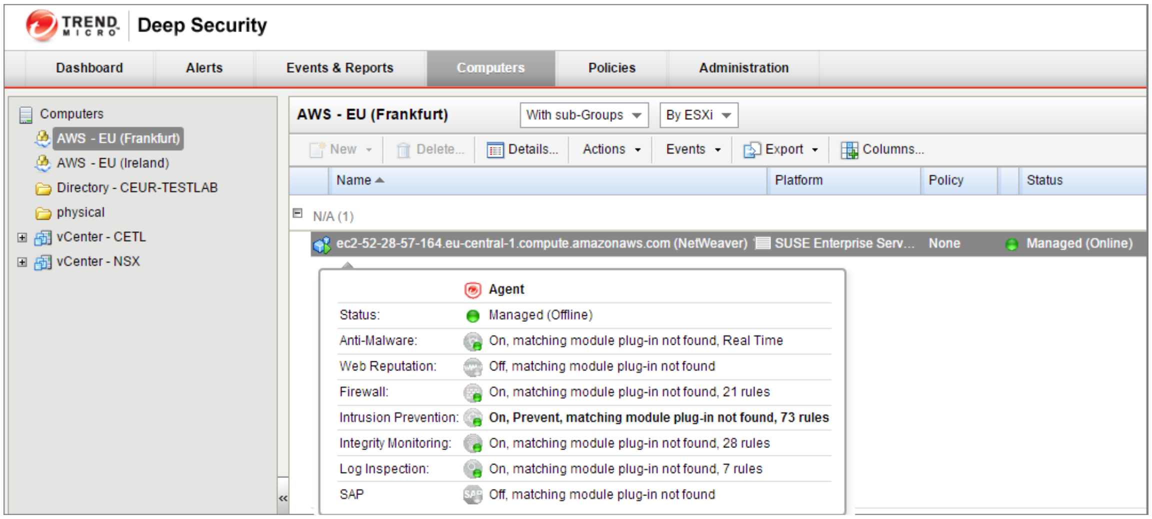
```
/opt/ds_agent/dsa_control -a dsm://cetl-dsm.ceur-testlab.trendmicro.de:4120/
```



```
ip-172-21-0-50:/home/ec2-user # rpm -ihv Agent-Core-SuSE_11-9.5.3-2774.x86_64.rpm
Preparing...                ########################################### [100%]
   1:ds_agent               ########################################### [100%]
Starting ds_agent:                                                    done
ip-172-21-0-50:/home/ec2-user # /opt/ds_agent/dsa_control -a dsm://cetl-dsm.ceur-testlab.trendmicro
.de:4120/
Starting thread 'CScriptThread' with stack size of 1048576
HTTP Status: 200 - OK
Response:
Attempting to connect to https://cetl-dsm.ceur-testlab.trendmicro.de:4120/
SSL handshake completed successfully - initiating command session.
Connected with AES256-SHA to peer at cetl-dsm.ceur-testlab.trendmicro.de
Received a 'GetHostInfo' command from the manager.
Received a 'GetHostInfo' command from the manager.
Received a 'SetDSMCert' command from the manager.
Received a 'SetAgentCredentials' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetInterfaces' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'SetSecurityConfiguration' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Command session completed.
ip-172-21-0-50:/home/ec2-user # 
```

This output indicates that the Agent activation is complete.

You can confirm the activation by checking the **Computers** tab in the Deep Security Manager console:



Name	Platform	Policy	Status
N/A (1)			
ec2-52-28-57-164.eu-central-1.compute.amazonaws.com (NetWeaver)	SUSE Enterprise Serv...	None	Managed (Online)

	Agent
Status:	Managed (Offline)
Anti-Malware:	On, matching module plug-in not found, Real Time
Web Reputation:	Off, matching module plug-in not found
Firewall:	On, matching module plug-in not found, 21 rules
Intrusion Prevention:	**On, Prevent, matching module plug-in not found, 73 rules**
Integrity Monitoring:	On, matching module plug-in not found, 28 rules
Log Inspection:	On, matching module plug-in not found, 7 rules
SAP	Off, matching module plug-in not found

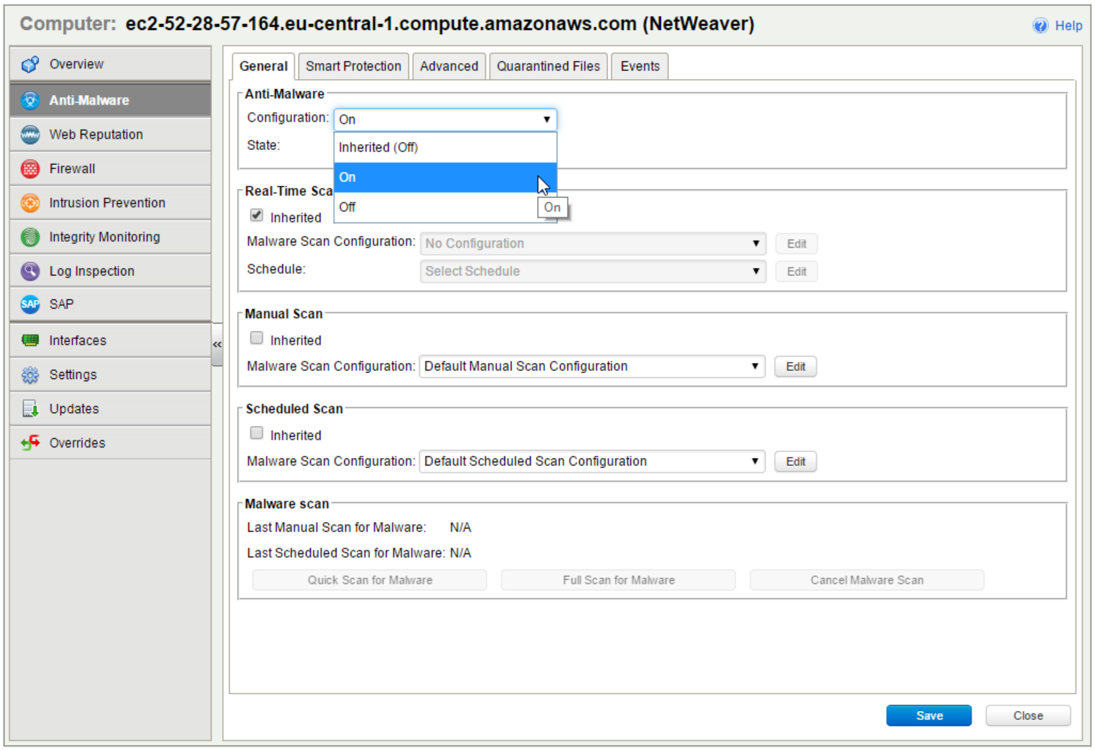
Assign a Security Profile

As shown in the image at the end of the previous section, the Agent is **Managed (Online)** but there is no protection module installed. This means that the Agent the Manager are communicating but the Agent is not using any configuration.

There are several ways to apply protection. In this example, the configuration is done directly on the SAP instance by activating Anti-Malware and SAP and assigning the default **Scan Configurations.**

To enable Anti-Malware and SAP functionality on a computer:

1. In the Computer editor, go to **Anti-Malware > General**.
2. In the **Anti-Malware** section, set **Configuration** to **On** (or **Inherited On**) and then click **Save**.



Computer: ec2-52-28-57-164.eu-central-1.compute.amazonaws.com (NetWeaver)

Anti-Malware
Configuration: On
State:

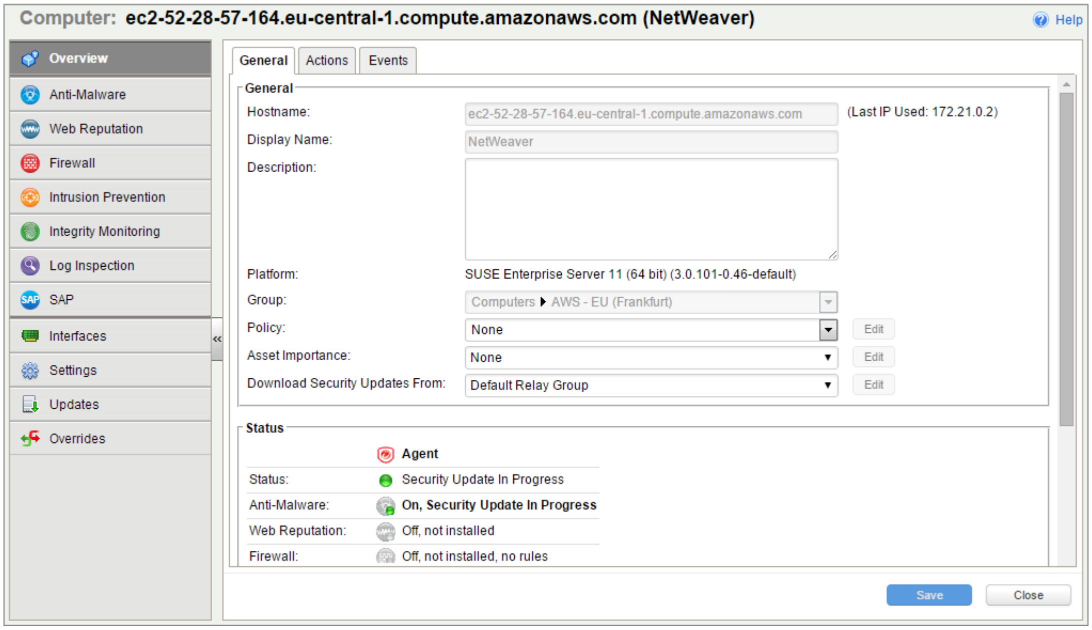
Real-Time Sca
☑ Inherited
Malware Scan Configuration: No Configuration
Schedule: Select Schedule

Manual Scan
□ Inherited
Malware Scan Configuration: Default Manual Scan Configuration

Scheduled Scan
□ Inherited
Malware Scan Configuration: Default Scheduled Scan Configuration

Malware scan
Last Manual Scan for Malware: N/A
Last Scheduled Scan for Malware: N/A

3. In the **Real-Time Scan**, **Manual Scan**, or **Scheduled Scan** sections, set the **Malware Scan Configuration** and **Schedule**, or allow those settings to be inherited from the parent policy.
4. Click **Save**. The status of the Anti-Malware module changes to **Off, installation pending**. This means that the Agent is retrieving the required module from the Deep Security Manager. For this to work, the client needs to access the **Deep Security Relay** on **TCP port 4122**. A few moments later, the Agent should start downloading security updates such as Anti-Malware patterns and scan engines:



Computer: ec2-52-28-57-164.eu-central-1.compute.amazonaws.com (NetWeaver)

General

Hostname: ec2-52-28-57-164.eu-central-1.compute.amazonaws.com (Last IP Used: 172.21.0.2)

Display Name: NetWeaver

Description:

Platform: SUSE Enterprise Server 11 (64 bit) (3.0.101-0.46-default)

Group: Computers ▸ AWS - EU (Frankfurt)

Policy: None

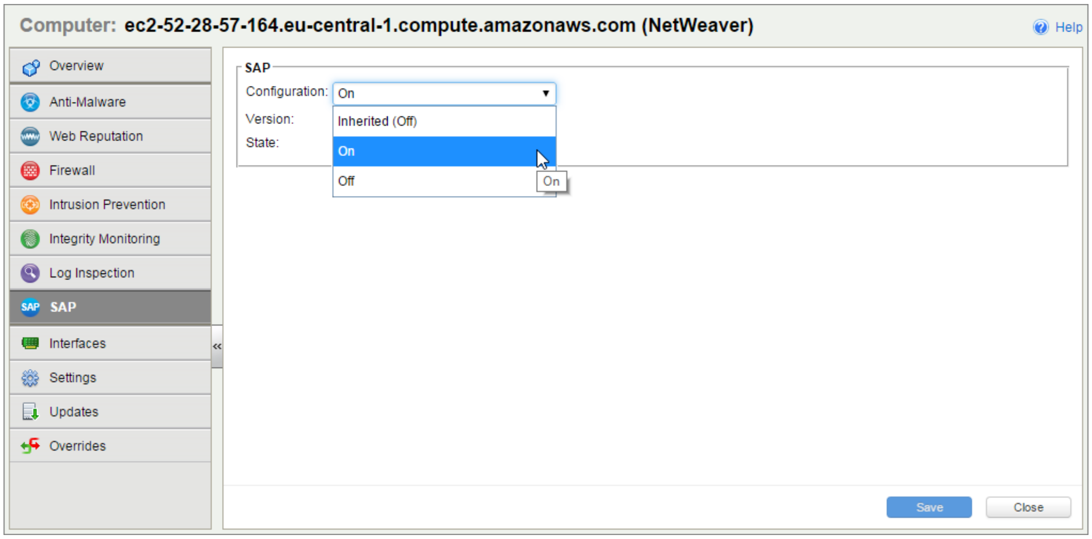
Asset Importance: None

Download Security Updates From: Default Relay Group

Status

	Agent
Status:	Security Update In Progress
Anti-Malware:	On, Security Update In Progress
Web Reputation:	Off, not installed
Firewall:	Off, not installed, no rules

5. In the Computer editor, go to **SAP**.
6. In the **SAP** section, set **Configuration** to **On** (or **Inherited On**) and then click **Save**:



Computer: ec2-52-28-57-164.eu-central-1.compute.amazonaws.com (NetWeaver)

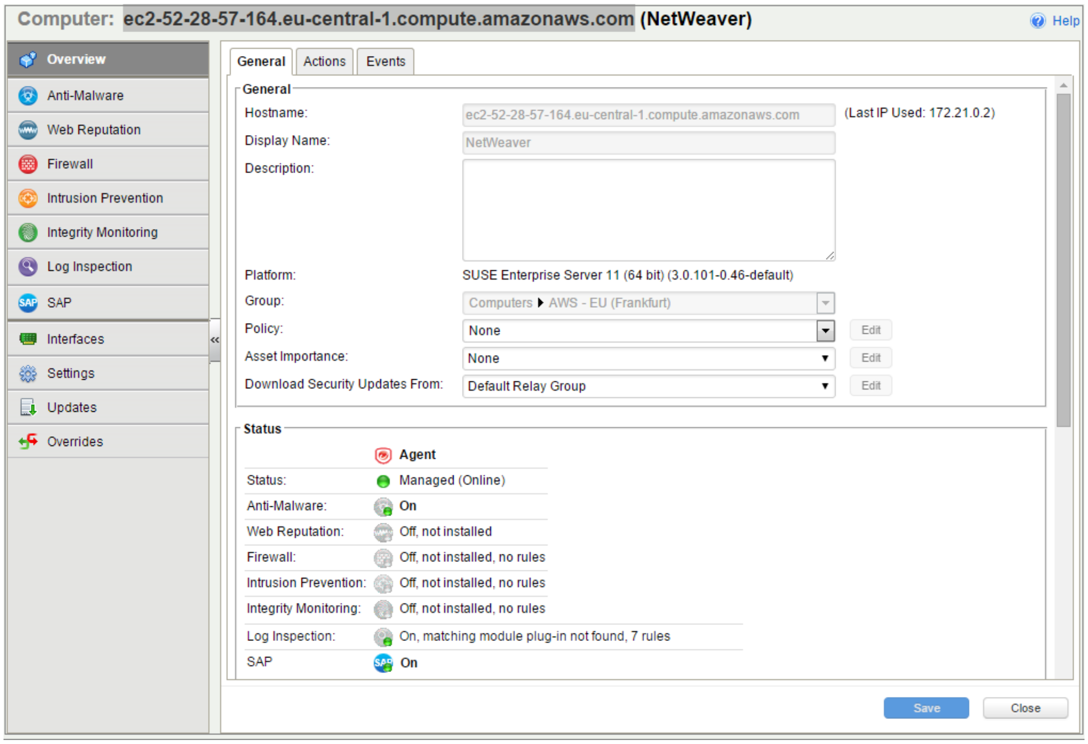
SAP

Configuration: On

Version:

State:

After status of the Agent changes to **Managed (Online)** again and the Anti-Malware and SAP modules are **On**, you can proceed with the SAP configuration.



Computer: ec2-52-28-57-164.eu-central-1.compute.amazonaws.com (NetWeaver)

General

Hostname: ec2-52-28-57-164.eu-central-1.compute.amazonaws.com (Last IP Used: 172.21.0.2)

Display Name: NetWeaver

Description:

Platform: SUSE Enterprise Server 11 (64 bit) (3.0.101-0.46-default)

Group: Computers ▸ AWS - EU (Frankfurt)

Policy: None

Asset Importance: None

Download Security Updates From: Default Relay Group

Status

	Agent
Status:	● Managed (Online)
Anti-Malware:	On
Web Reputation:	Off, not installed
Firewall:	Off, not installed, no rules
Intrusion Prevention:	Off, not installed, no rules
Integrity Monitoring:	Off, not installed, no rules
Log Inspection:	On, matching module plug-in not found, 7 rules
SAP	On

Configure SAP to Use the Deep Security Agent

The Deep Security Agent is now up and running and is able to scan the file system of its operating system. Next, we need to make the Agent aware of the SAP application server. To use this, we must create a *Virus Scan Adapter* inside the application server. The virus scan adapter must be part of a group, mainly for load balancing purposes. After the virus scan adapter and virus scan group are created, we can use Virus Scan Profiles to configure what to scan and how to behave.

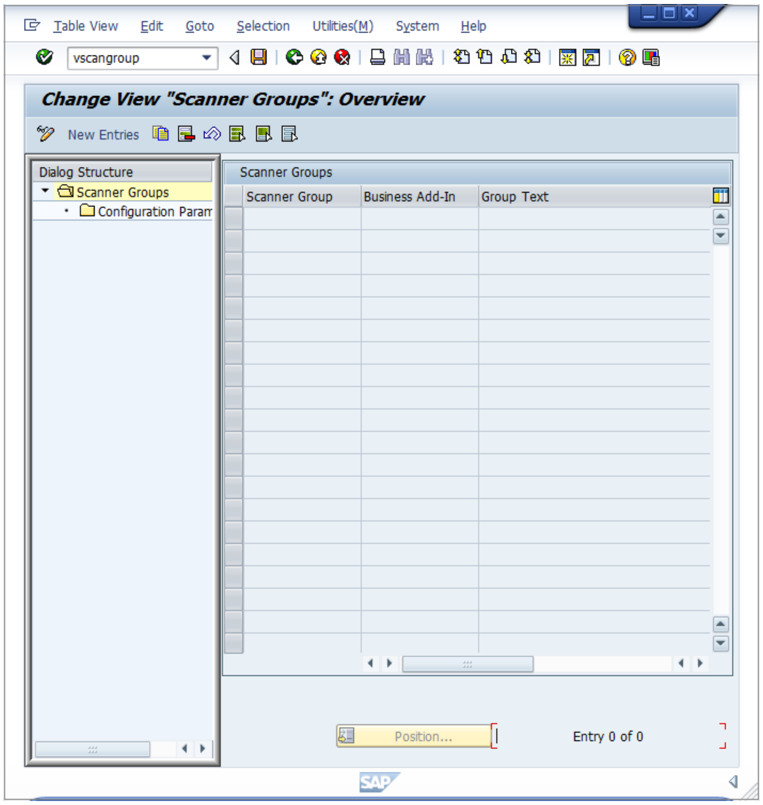
These are the required steps:

1. Configure the Trend Micro Scanner Group
2. Configure the Trend Micro Virus Scan Provider
3. Configure the Trend Micro Virus Scan Profile
4. Test the Virus Scan Interface

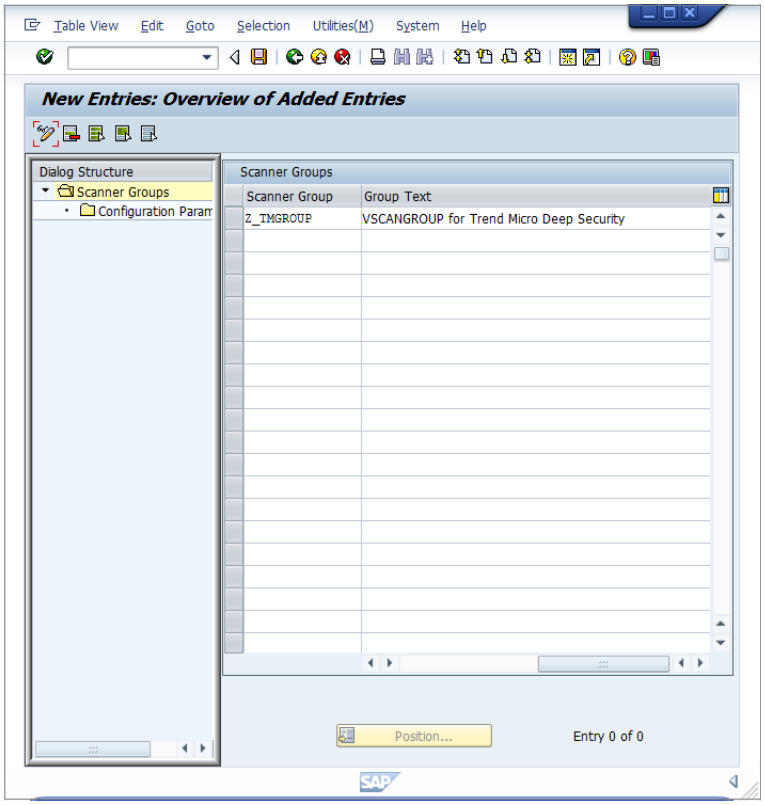
Note: *The virus scan group and the virus scan adapter are both global configurations (client 00). The virus scan profile must be configured in each tenant (client 01, 02, etc.).*

Configure the Trend Micro Scanner Group

1. In the SAP WinGUI, run the **VSCANGROUP** transaction.



2. In Edit mode, click **New Entries**. Create a new scanner group, specifying a group name in the **Scanner Group** area and a description of the scanner group in the **Group Text** area.

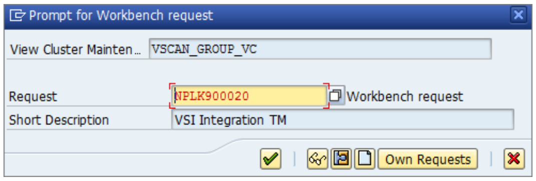


New Entries: Overview of Added Entries

Scanner Groups

Scanner Group	Group Text
Z_TMGROUP	VSCANGROUP for Trend Micro Deep Security

3. Clicking **Save** or leaving the edit mode will prompt you to commit a “workbench request”. In this example, a new workbench request is created to keep track of all the VSI-related changes:

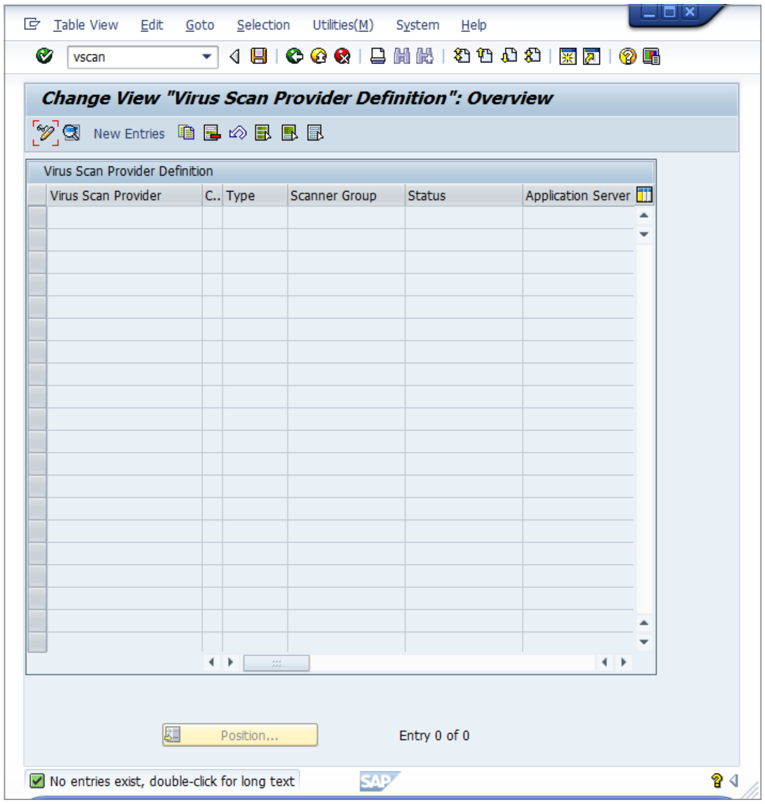


View Cluster Mainten...	VSCAN_GROUP_VC
Request	NPLK900020 Workbench request
Short Description	VSI Integration TM

The next step is the actual configuration of the VSI integration. It is called a **Virus Scan Adapter**.

Configure the Trend Micro Virus Scan Provider

1. In the SAP WinGUI, run the **VSCAN** transaction.



Change View "Virus Scan Provider Definition": Overview

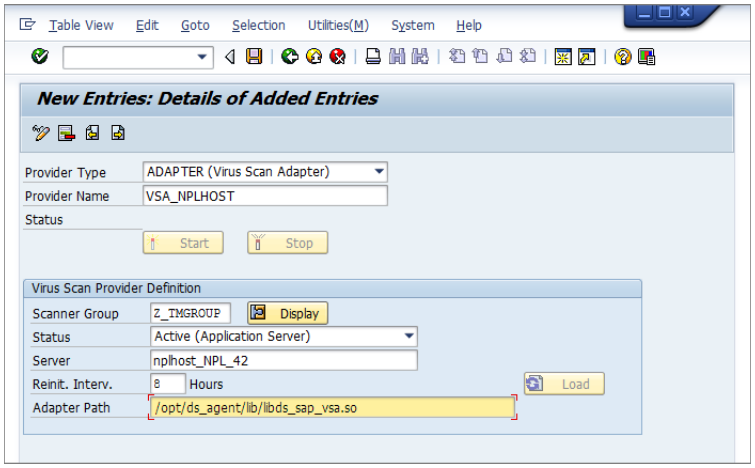
Virus Scan Provider Definition

Virus Scan Provider	C..	Type	Scanner Group	Status	Application Server

Entry 0 of 0

No entries exist, double-click for long text

2. In Edit mode, click **New Entries**. Creating a new entry displays a prompt in which the configuration of the VSI-certified solution takes place. In this example, the following configuration parameters are set:



New Entries: Details of Added Entries

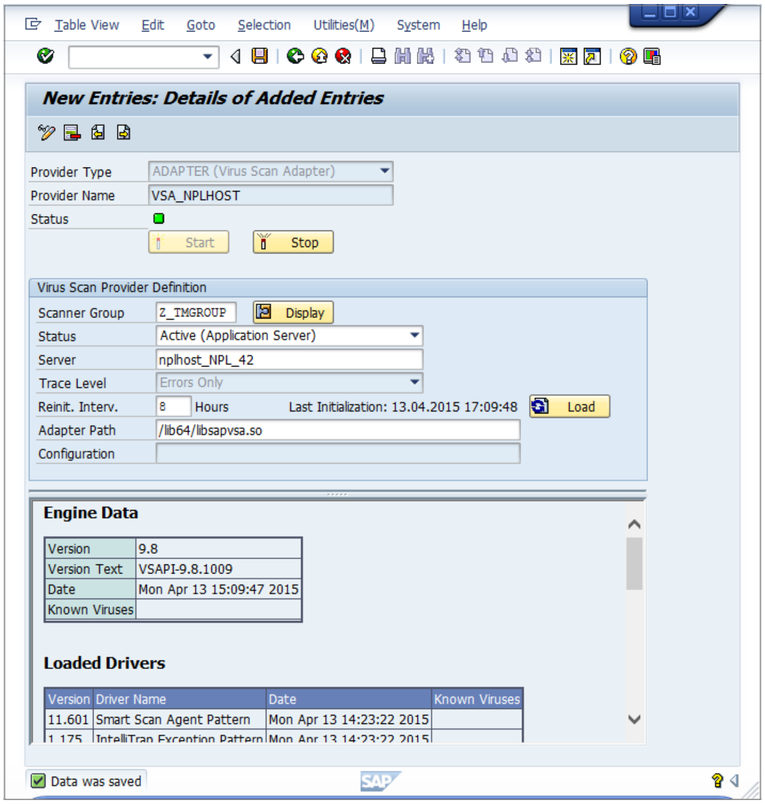
Provider Type: ADAPTER (Virus Scan Adapter)
Provider Name: VSA_NPLHOST
Status

Virus Scan Provider Definition
Scanner Group: Z_TMGROUP
Status: Active (Application Server)
Server: nplhost_NPL_42
Reinit. Interv.: 8 Hours
Adapter Path: /opt/ds_agent/lib/libds_sap_vsa.so

Setting	Value	Description
Provider Type:	ADAPTER (Virus Scan Adapter)	Automatically set (default)
Provider Name:	VSA_<host name>	Automatically set, serves as alias
Scanner Group:	Select the group that you configured earlier	All previously created scanner groups, which you can display using the input help
Status:	Active (Application Server)	Automatically set (default)
Server:	nplhost_NPL_42	Automatically set, hostname
Reinit. Interv.:	8 Hours	Specifies the number of hours after which the Virus Scan Adapter will be reinitialized and load new virus definitions.

Setting	Value	Description
Adapter Path:	/opt/ds_agent/lib/libds_sap_vsa.so	This is the default path.

3. When you click **Save** or leave the edit mode, there is another prompt to pack this into a workbench request. After confirming, click the **Start** button. The Status light will turn green, which means the adapter is loaded and active:



New Entries: Details of Added Entries

Provider Type	ADAPTER (Virus Scan Adapter)
Provider Name	VSA_NPLHOST
Status	🟩

Virus Scan Provider Definition

Scanner Group	Z_TMGROUP
Status	Active (Application Server)
Server	nplhost_NPL_42
Trace Level	Errors Only
Reinit. Interv.	8 Hours Last Initialization: 13.04.2015 17:09:48
Adapter Path	/lib64/libsapvsa.so
Configuration	

Engine Data

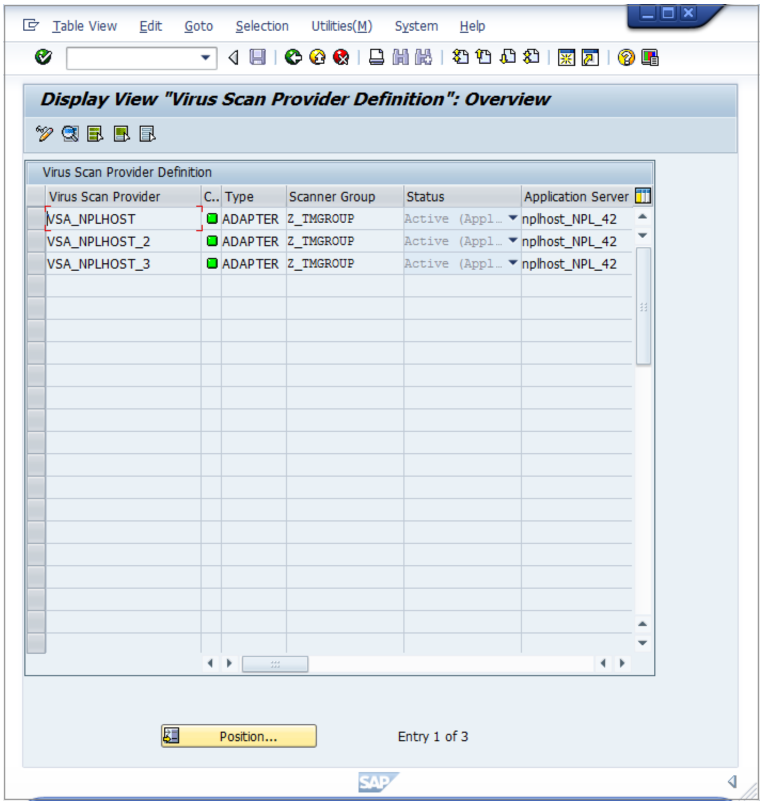
Version	9.8
Version Text	VSAPI-9.8.1009
Date	Mon Apr 13 15:09:47 2015
Known Viruses	

Loaded Drivers

Version	Driver Name	Date	Known Viruses
11.601	Smart Scan Agent Pattern	Mon Apr 13 14:23:22 2015	
1.175	IntelliTrap Exception Pattern	Mon Apr 13 14:23:22 2015	

☑ Data was saved

4. It is recommended to repeat this step 2 to 3 times to have multiple threads so that the VSCANGROUP can load balance file transactions:



Display View "Virus Scan Provider Definition": Overview

Virus Scan Provider Definition

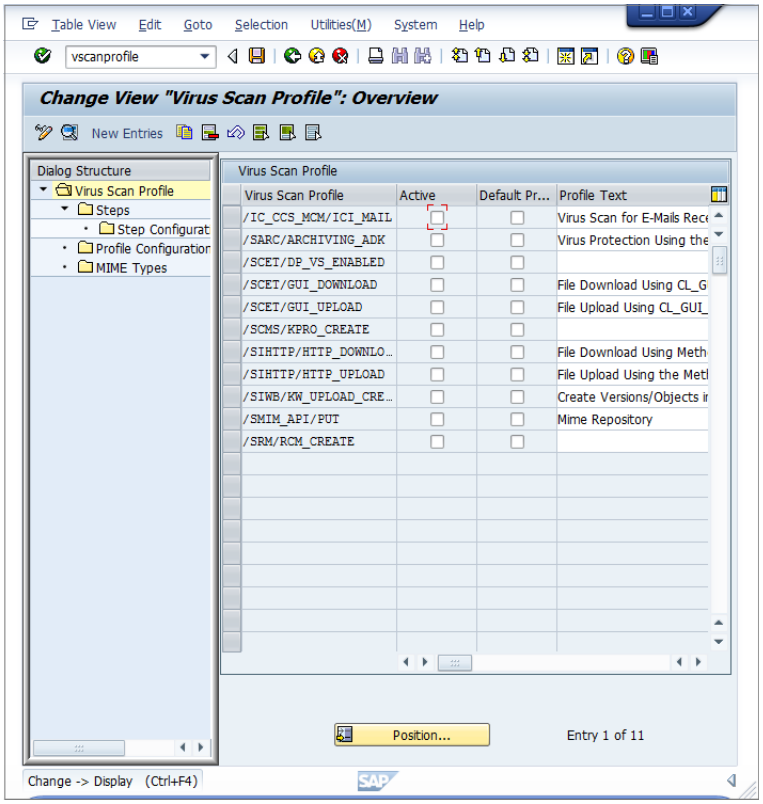
Virus Scan Provider	C..	Type	Scanner Group	Status	Application Server
VSA_NPLHOST	🟩	ADAPTER	Z_TMGROUP	Active (Appl…	nplhost_NPL_42
VSA_NPLHOST_2	🟩	ADAPTER	Z_TMGROUP	Active (Appl…	nplhost_NPL_42
VSA_NPLHOST_3	🟩	ADAPTER	Z_TMGROUP	Active (Appl…	nplhost_NPL_42

Entry 1 of 3

At this point, the VSI configuration is nearly finished. The application server is now ready to process file transactions using a virus scan provided by Trend Micro Deep Security.

Configure the Trend Micro Virus Scan Profile

1. In the SAP WinGUI, run the **VSCANPROFILE** transaction.



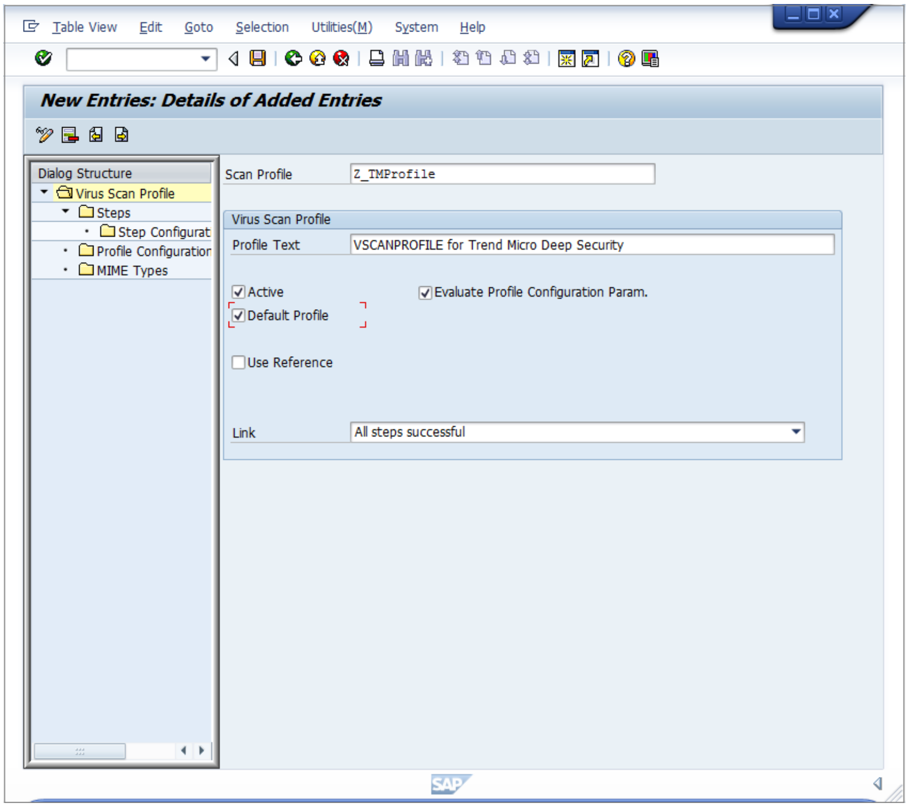
Change View "Virus Scan Profile": Overview

Virus Scan Profile

Virus Scan Profile	Active	Default Pr...	Profile Text
/IC_CCS_MCM/ICI_MAIL	□	□	Virus Scan for E-Mails Rece
/SARC/ARCHIVING_ADK	□	□	Virus Protection Using the
/SCET/DP_VS_ENABLED	□	□	
/SCET/GUI_DOWNLOAD	□	□	File Download Using CL_G
/SCET/GUI_UPLOAD	□	□	File Upload Using CL_GUI_
/SCMS/KPRO_CREATE	□	□	
/SIHTTP/HTTP_DOWNLO...	□	□	File Download Using Meth
/SIHTTP/HTTP_UPLOAD	□	□	File Upload Using the Metl
/SIWB/KW_UPLOAD_CRE...	□	□	Create Versions/Objects ir
/SMIM_API/PUT	□	□	Mime Repository
/SRM/RCM_CREATE	□	□	

Entry 1 of 11

2. In Edit mode, click **New Entries**. The virus scan profiles will define how specific transactions (file uploads, file downloads, etc.) are handled corresponding to the virus scan interface. To have the previously configured virus scan adapter used in the application server, a new virus scan profile needs to be created:



New Entries: Details of Added Entries

Dialog Structure
- Virus Scan Profile
  - Steps
    - Step Configurat
  - Profile Configuration
  - MIME Types

Scan Profile: Z_TMProfile

Virus Scan Profile

Profile Text: VSCANPROFILE for Trend Micro Deep Security

☑ Active ☑ Evaluate Profile Configuration Param.

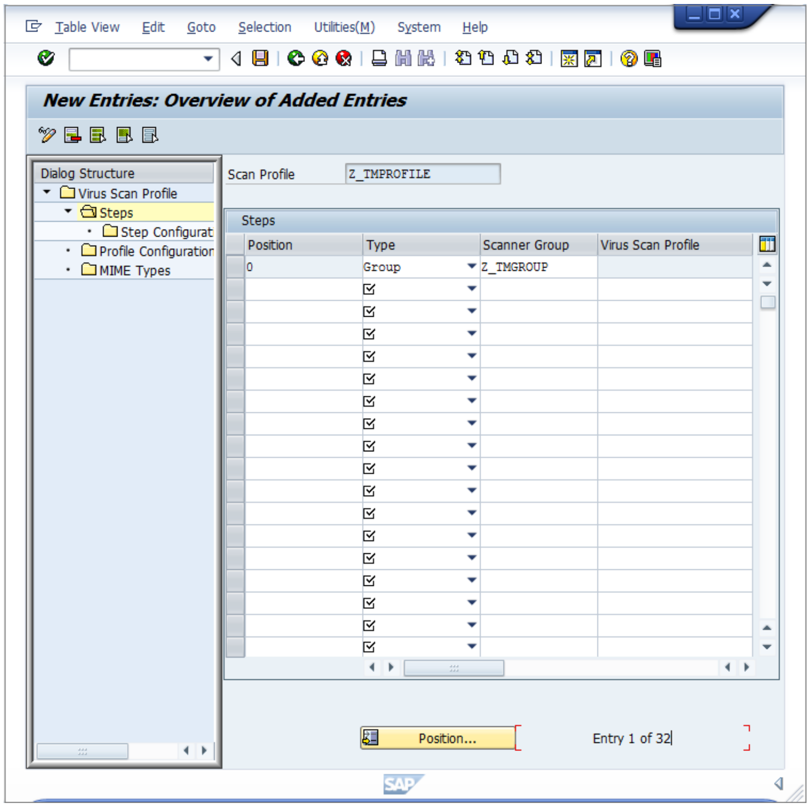
☑ Default Profile

□ Use Reference

Link: All steps successful

3. In the **Scan Profile** box, enter "Z_TMProfile" and select the **Active**, **Default Profile**, and **Evaluate Profile Configuration Param.** checkboxes.

4. While still in edit mode, double-click **Steps** to configure the steps:



New Entries: Overview of Added Entries

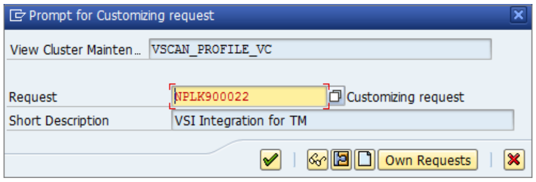
Scan Profile Z_TMPROFILE

Steps

Position	Type	Scanner Group	Virus Scan Profile
0	Group	Z_TMGROUP	

Entry 1 of 32

5. Click **New Entries**.
6. The steps define what to do when the profile is called by a transaction. Set the **Position** to "0", **Type** to "Group" and the **Scanner Group** to the name of the group that you configured earlier.
7. After clicking **Save** or leaving the edit mode, you will eventually receive a notification about an existing virus scan profile, **/SCET/DP_VS_ENABLED**. you can ignore this notification because the profile is not active and is not used. After confirming this notification, you will be asked to pack this configuration in a “customization request”. Creating a new request will help keep track of the changes that have been made:



Prompt for Customizing request

View Cluster Mainten... VSCAN_PROFILE_VC

Request NPLK900022 Customizing request

Short Description VSI Integration for TM

8. To create configuration parameters for a step, double-click the **Profile Configuration Parameters** node. Click **New Entries** and set the parameters:

Parameter	Type	Description
CUST_ACTIVE_CONTENT	BOOL	Check whether a file contains script (Java/PHP/ASP script) and block
CUST_CHECK_MIME_TYPE	BOOL	Check whether the file extension name matches its MIME type. If they do not match, the file will be blocked. All MIME types and extension names can be exactly matched. For example: ◦ Word files must to be .doc or .dot ◦ JPEG files must to be .jpg ◦ Text and binary files could be any extension (won’t block)

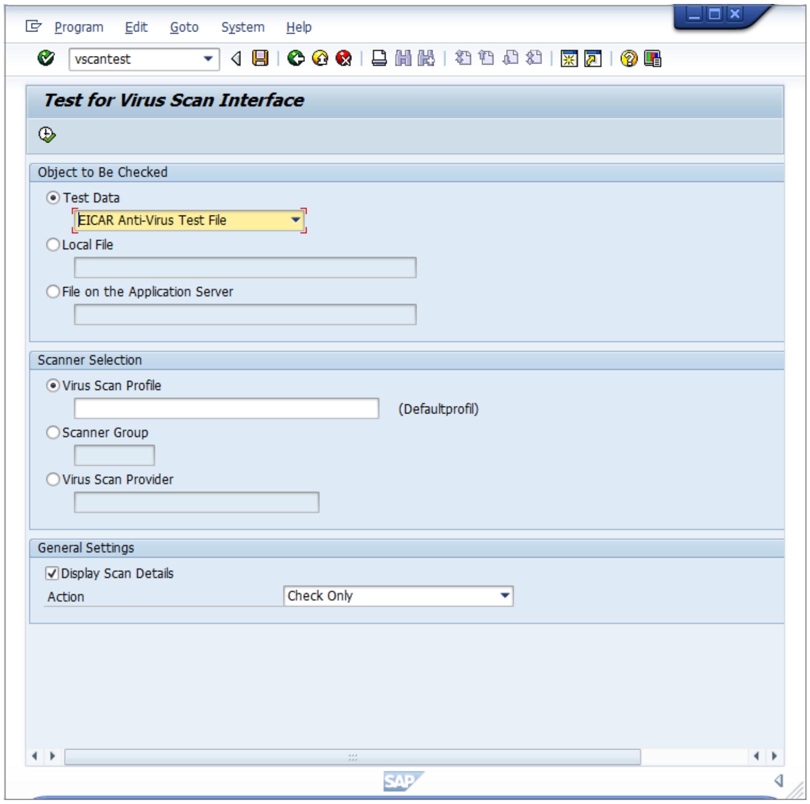
9. Double-click the **Step Configuration Parameters** node. Click **New Entries** and set the parameters:

Parameter	Type	Description
SCANBESTEFFORT	BOOL	The scan should be performed on the "best effort" basis; that is, all (security critical) flags that allow a VSA to scan an object should be activated, such as SCANALLFILES and SCANEXTRACT, but also internal flags. Details about exactly which flags these are can be stored in the certification.
SCANALLFILES	BOOL	Scans for all files regardless of their file extension.
SCANEXTENSIONS	CHAR	List of the file extensions for which the VSA should scan. Only files with the configured extensions will be checked. Other extensions are blocked. Wildcards can also be used here in order to search for patterns. * stands for this location and following and ? stands for for only this character. The syntax is: exe;com;do?;ht* => `*` therefore means to scan all files.
SCANLIMIT	INT	This settings applies to compressed files. It specifies the maximum number of files that will be unpacked and scanned.
SCANEXTRACT	BOOL	Archives or compressed objects are to be unpacked
SCANEXTRACT_SIZE	SIZE_T	Maximum unpack size
SCANEXTRACT_DEPTH	INT	Maximum depth to which an object is to be unpacked.
SCANMIMETYPES	CHAR	List of the MIME types to be scanned for. Only files with configured MIME types will be checked. Other MIME types are blocked. This parameter works only if CUST_CHECK_MIME_TYPE is enabled.
BLOCKMIMETYPES	CHAR	List of MIME types to be used as black list (they will be blocked). This parameter works only if CUST_CHECK_MIME_TYPE is enabled.
BLOCKEXTENSIONS	CHAR	List of file extensions to be used as black list

This configuration is per-client, so it must be done in each tenant of the SAP application server.

Test the Virus Scan Interface

1. In the SAP WinGUI, run the **VSCANTEST** transaction.



vscantest

Test for Virus Scan Interface

Object to Be Checked

● Test Data

EICAR Anti-Virus Test File

○ Local File

○ File on the Application Server

Scanner Selection

● Virus Scan Profile (Defaultprofil)

○ Scanner Group

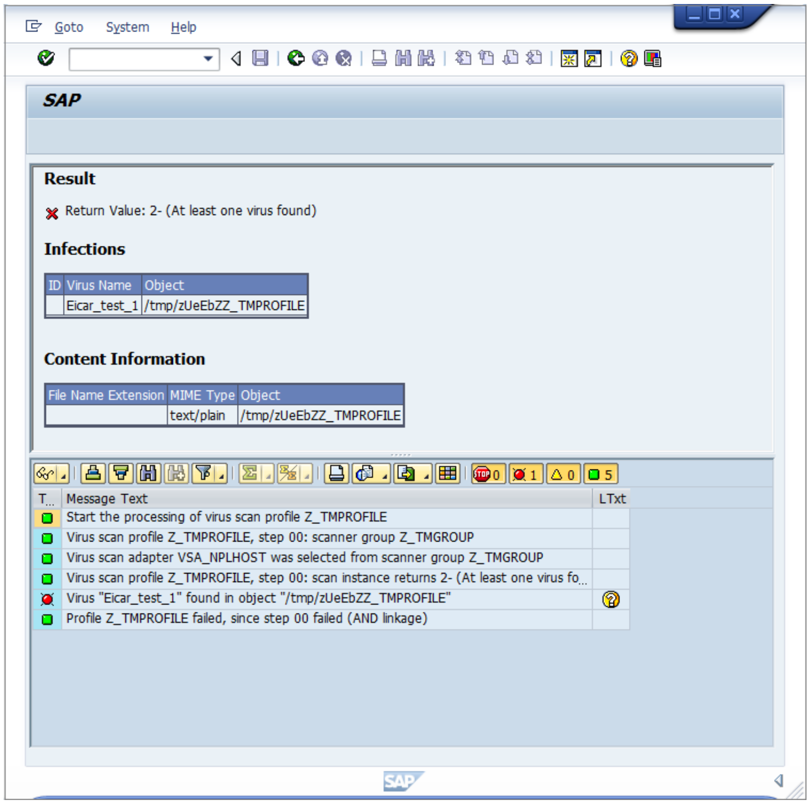
○ Virus Scan Provider

General Settings

☑ Display Scan Details

Action: Check Only

2. Every VSI-aware SAP application server also has a built-in test to check whether the configuration steps were done correctly. For this, an EICAR test virus (www.eicar.org) is packed in a transaction that can call a specific scanner. Not filling in anything will call the default profile, which was configured in the last step.
3. Clicking **Execute** prompts a notification that explains what an EICAR test virus is. After confirming this, you will see how the transaction is intercepted:



Result

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

Infections

ID	Virus Name	Object
	Eicar_test_1	/tmp/zUeEbZZ_TMPROFILE

Content Information

File Name Extension	MIME Type	Object
	text/plain	/tmp/zUeEbZZ_TMPROFILE

T...	Message Text	LTxt
🟩	Start the processing of virus scan profile Z_TMPROFILE	
🟩	Virus scan profile Z_TMPROFILE, step 00: scanner group Z_TMGROUP	
🟩	Virus scan adapter VSA_NPLHOST was selected from scanner group Z_TMGROUP	
🟩	Virus scan profile Z_TMPROFILE, step 00: scan instance returns 2- (At least one virus fo...	
●	Virus "Eicar_test_1" found in object "/tmp/zUeEbZZ_TMPROFILE"	?
🟩	Profile Z_TMPROFILE failed, since step 00 failed (AND linkage)	

Infections shows information about the detected malware.

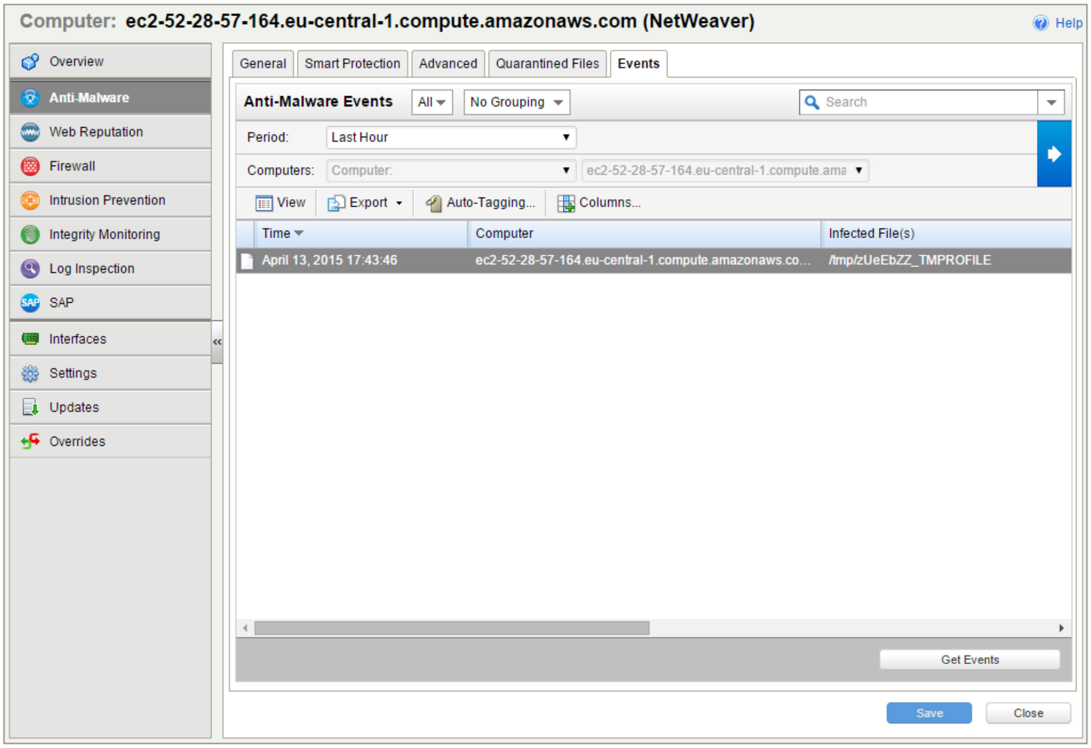
Content Information shows the correct MIME-type of the file.

The file name is always a randomly generated 7-letter alphabetic string followed by the virus scan profile name.

After this, there is an output about each step of the transaction:

1. The transaction called the default virus scan profile, which is the virus scan profile **Z_TMPROFILE**.
2. The virus scan profile **Z_TMPROFILE** is configured to call an adapter from the virus scan group **Z_TMGROUP**.
3. The virus scan group **Z_TMGROUP** has multiple adapters configured and calls one of them (in this case, **VSA_NPLHOST**).
4. The virus scan adapter returns value **2-**, which means a virus was found.
5. Information about the detected malware is displayed by showing **Eicar_test_1** and the file object **/tmp/zUeEbZZ_TMPROFILE**.
6. The called default virus scan profile **Z_TMPROFILE** fails because step 00 (the virus scan group) was not successful and therefor the file transaction is stopped from further processing.

For a cross-check, there is also information about this “malware”-event in the Deep Security Manager console:



Computer: ec2-52-28-57-164.eu-central-1.compute.amazonaws.com (NetWeaver)

Period: Last Hour

Computers: Computer: ec2-52-28-57-164.eu-central-1.compute.ama

Time	Computer	Infected File(s)
April 13, 2015 17:43:46	ec2-52-28-57-164.eu-central-1.compute.amazonaws.co...	/tmp/zUeEbZZ_TMPROFILE

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM96985/150612