10 Protecting against malware with ClamSAP

ClamSAP integrates the ClamAV anti-malware toolkit into SAP NetWeaver and SAP Mobile Platform applications. ClamSAP is a shared library that links between ClamAV and the SAP NetWeaver Virus Scan Interface (NW-VSI). The version of ClamSAP shipped with SUSE Linux Enterprise Server for SAP Applications 15 SP3 supports NW-VSI version 2.0.

10.1 Installing ClamSAP

1. On the application host, install the packages for ClamAV and ClamSAP. To do so, use the command:

   ```
   tux > sudo zypper install clamav clamsap
   ```

2. Before you can enable the daemon `clamd`, initialize the malware database:

   ```
   tux > sudo freshclam
   ```

3. Start the service `clamd`:

   ```
   tux > sudo systemctl start clamd
   ```

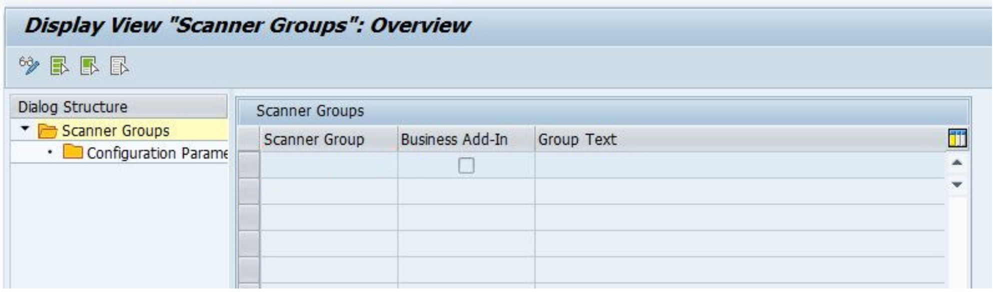
4. Check the status of the service `clamd` with:

   ```
   tux > systemctl status clamd
   ● clamd.service - ClamAV Antivirus Daemon
   Loaded: loaded (/usr/lib/systemd/system/clamd.service; enabled; vendor preset:
    disabled)
   Active: active (running) since Tue 2017-04-11 10:33:03 UTC; 24h ago
   [...]
   ```

10.2 Creating a virus scanner group in SAP NetWeaver

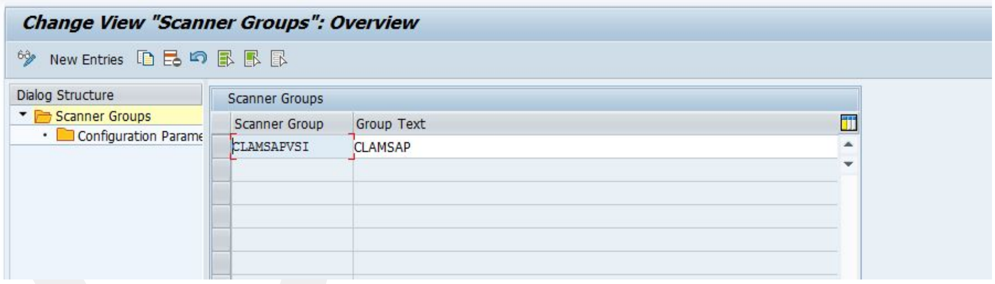
1. Log in to the SAP NetWeaver installation through the GUI. Do not log in as a `DDIC` or `SAP*` user, because the virus scanner needs to be configured cross-client.

2. Create a Virus Scanner Group using the transaction *VSCANGROUP*.



3. To switch from view mode to change mode, click the button *Change View* (✎).
   Confirm the message *This table is cross-client* by clicking the check mark. The table is now editable.

4. Select the first empty row. In the text box *Scanner Group*, specify `CLAMSAPVSI`. Under *Group Text*, specify `CLAMSAP`.
   Make sure that *Business Add-in* is not checked.



Scanner Group	Group Text
CLAMSAPVSI	CLAMSAP

5. To save the form, click the button *Save* (💾).

10.3 Setting up the ClamSAP library in SAP NetWeaver

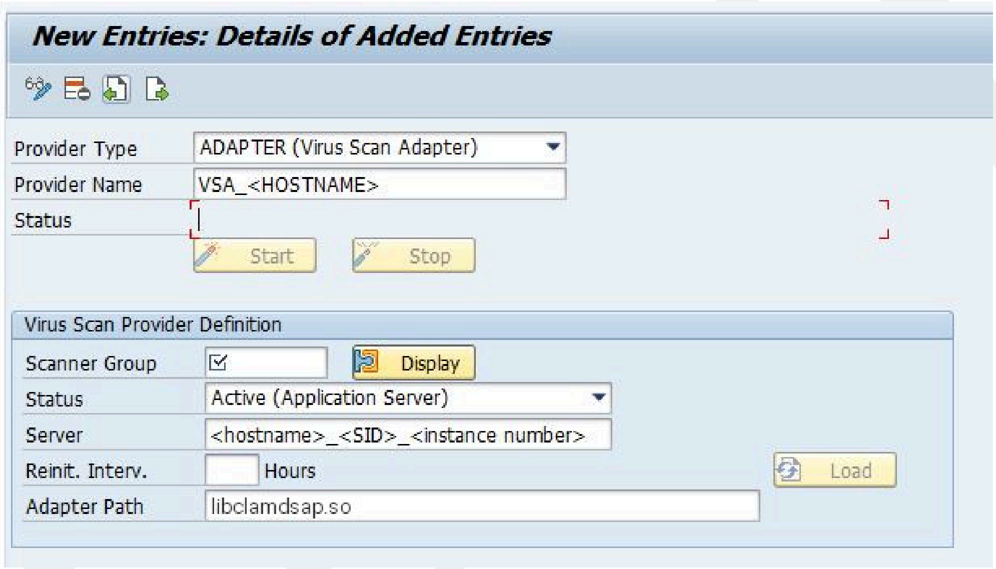
1. In the SAP NetWeaver GUI, call the transaction *VSCAN*.

2. To switch from view mode to change mode, click the button *Change View* (✎).
   Confirm the message *This table is cross-client* by clicking the check mark. The table is now editable.

3. Click *New entries*.

4. Fill in the form accordingly:

    - *Provider Type*: `Adapter (Virus Scan Adapter)`
    - *Provider Name*: `VSA_HOSTNAME` (for example: `VSA_SAPSERVER`)
    - `Scanner Group`: The name of the scanner group that you set up in *Section 10.2, “Creating a virus scanner group in SAP NetWeaver”* (for example: `CLAMSAPVSI`)
    - *Server*: `HOSTNAME_SID_INSTANCE_NUMBER` (for example: `SAPSERVER_P04_00`)
    - *Adapter Path*: `libclamdsap.so`



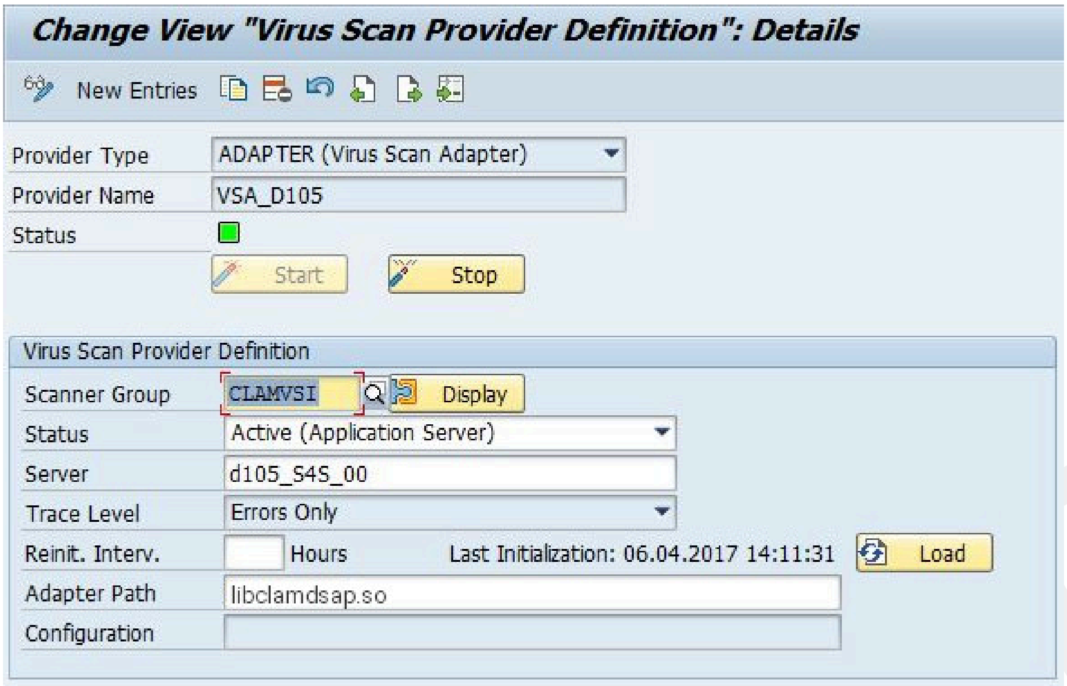
New Entries: Details of Added Entries
Start
Stop
Virus Scan Provider Definition
Display
Load

Provider Type	ADAPTER (Virus Scan Adapter)
Provider Name	VSA_<HOSTNAME>
Status	
Scanner Group	☑
Status	Active (Application Server)
Server	<hostname>_<SID>_<instance number>
Reinit. Interv.	Hours
Adapter Path	libclamdsap.so

5. To save the form, click the button 💾.

10.4 Engaging ClamSAP

To run ClamSAP, go to the transaction *VSCAN*. Then click *Start*.



Change View "Virus Scan Provider Definition": Details

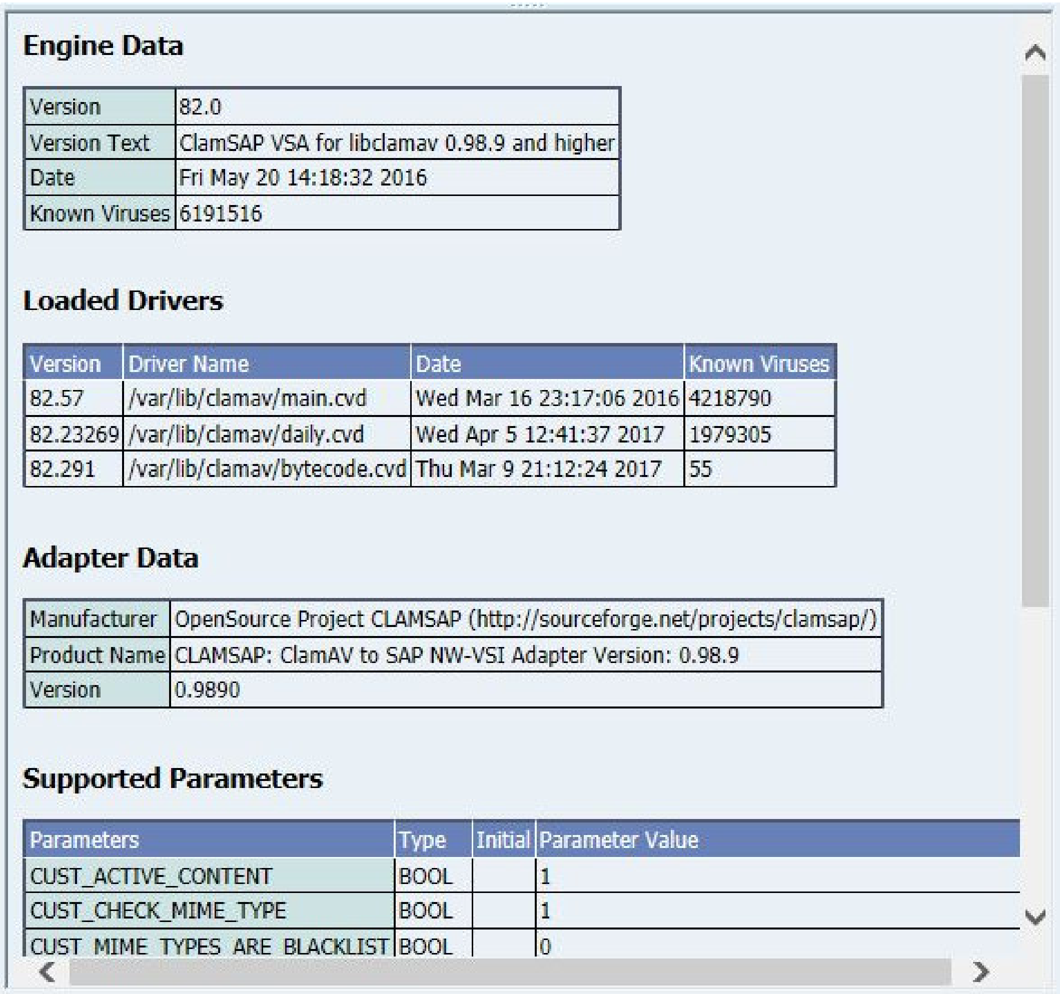
Provider Type: ADAPTER (Virus Scan Adapter)
Provider Name: VSA_D105
Status: 🟩

Virus Scan Provider Definition

Scanner Group: CLAMVSI
Status: Active (Application Server)
Server: d105_S4S_00
Trace Level: Errors Only
Reinit. Interv.: Hours
Last Initialization: 06.04.2017 14:11:31
Adapter Path: libclamdsap.so
Configuration:

FIGURE 10.1: CHANGE VIEW “VIRUS SCAN PROVIDER DEFINITION”

Afterward, a summary will be displayed, including details of the ClamSAP and ClamAV (shown in *Figure 10.2, “Summary of ClamSAP data”*).



Engine Data

Version	82.0
Version Text	ClamSAP VSA for libclamav 0.98.9 and higher
Date	Fri May 20 14:18:32 2016
Known Viruses	6191516

Loaded Drivers

Version	Driver Name	Date	Known Viruses
82.57	/var/lib/clamav/main.cvd	Wed Mar 16 23:17:06 2016	4218790
82.23269	/var/lib/clamav/daily.cvd	Wed Apr 5 12:41:37 2017	1979305
82.291	/var/lib/clamav/bytecode.cvd	Thu Mar 9 21:12:24 2017	55

Adapter Data

Manufacturer	OpenSource Project CLAMSAP (http://sourceforge.net/projects/clamsap/)
Product Name	CLAMSAP: ClamAV to SAP NW-VSI Adapter Version: 0.98.9
Version	0.9890

Supported Parameters

Parameters	Type	Initial	Parameter Value
CUST_ACTIVE_CONTENT	BOOL		1
CUST_CHECK_MIME_TYPE	BOOL		1
CUST_MIME_TYPES_ARE_BLACKLIST	BOOL		0

FIGURE 10.2: SUMMARY OF CLAMSAP DATA

10.5 For more information

For more information, also see the project home page https://sourceforge.net/projects/clamsap/ ↗.