Avira AntiVir Server for UNIX

HowTo

AVIRA

Table of contents

1. Implementation possibilities

- Local virus protection
- Samba server
- FTP Server
- NFS Server
- NSS Server
- Web server
- Email scanner (In combination with Amavis)

In this case you have to mount the corresponding shares with DazukoFS
(or configure the shares as an include path in Dazuko2)

Note
For the installation with Amavis, please, note the corresponding documentation of the Amavis projekt.
You can use the Avira Server Security for Unix with (OnAccess) or without real time protection (OnDemand).

2. Installation

2.1. Manually installation

- Decompress
  `gzip -d antivir-server-prof-3.0.2-5.tar.gz`
- Unpack
  `tar -xvf antivir-server-prof-3.0.2-5.tar`
- Change directory
  `cd antivir-server-prof-3.0.2-5`
- Execute installation
  `./install`
- Follow the installation dialog

The following requests are recommended and should be adopted

- Would you like to setup Engine and Signature updates as cron task ? [y]
- Please specify the interval to check. Recommended values are daily or 2 hours. available options: d [2]

- Please specify if boot scripts should be set up.
  Set up boot scripts [y]

> **Note**
> Please consider that the installation of the real time protection with Unix needs the external kernel module Dazuko 3.0.
> You find more information on the dazuko homepage.

2.2. Unattended Installation

If you want to perform a completely automatic (unattended) installation, you can use the installation type of the SMC while using the setup.inf which is part of the installation package:

```
$ ./install --fast --inf=./smcpkg/setup.inf
```

All settings for the automatic installation are located in the given INF file. You could use a copy of your own settings and e.g. proceed a larger rollout or simplify your daily work.

```
./smcpkg/setup.inf:
GUARD_INSTALL=y
GUARD_ADDLINK=y
GUARD_AUTOSTART=y
GUARD_STARTNOW=y
UPDATER_INSTALL=y
UPDATER_ADDLINK=y
UPDATER_AUTOSTART=ignore
GUI_INSTALL=y
DAZUKO_INSTALLTYPE=k
USE_DAZUKO_LIB=2
SAVAPI3_ADDLINK=y
UPDATER_INSTALL=y
UPDATER_ADDLINK=y
UPDATER_ADDCRONJOB=y
UPDATER_CYCLE_SIG_EN=2h
UPDATER_CYCLE_PROD=y
UPDATER_CYCLE=2
UPDATER_EMAILTO=n
SMC_INSTALL=y
ANTIVIR_CONFIG=n
LICENSE_AGREEMENT=y
WRITE_FSTAB=w
INST_DAZUKO=y
```

```
REPLACE_CRONJOB=n
REPLACE_CRONJOB_PRODUCT=n
GNOME_INSTALL=n
CONTINUE_IF_DAZUKO_FAILED=n
USE_DAZUKO2_IF_AVAILABLE=y
INST_DAZUKO=y
CREATE_QUAR_SMC=y
BIT_SUPPORT=n
FIREFOX_INSTALL=y
```

3. Recommended Basic Configuration

- **Amount of scanner daemons**

  ```
  NumDaemons 3
  ```

  This triggers the start of 3 daemons which are sufficient for a regular operation. The amount can be increased at a high workload. Please note that there should be enough memory available in such a case.

- **Action in case of detection**

  ```
  AlertAction quarantine
  ```

  in case of a detection the file will be moved to the quarantine directory and renamed. Therefore, the file will no longer be accessible for the user. However, the file will neither be deleted nor changed in the case of a false positive.

- **Default: QuarantineDirectory NONE**

  ```
  QuarantineDirectory/home/quarantine
  ```

  If a file from the /home directory has to be moved into quarantine, it is advisable for performance reasons to set this here.
  Instead of copying a large file from one partition to another, the file can simply be moved on the same partition.

- **Files to be checked**

  ```
  ScanMode all
  ```

  This mode scans all files.

- **Archive scan**

  ```
  ArchiveScan yes
  ```

  Activates the scan of small and medium archives. Large archives should be limited because of the performance. (view below)
  You can scan large archives e.g. by means of a regular scan.

- **Scan in mbox**

  ```
  MailboxScan yes
  ```

  This command executes a scan of the mail boxes. We recommend to activate this option for security reasons.

- **Maximum archive size which should be scanned**

  ```
  ArchiveMaxSize 1GB
  ```

  You should limit the size of archives which should be scanned to 1 GB for a good performance.

- **Maximum recursion depth**

  ```
  ArchiveMaxRecursion 20
  ```

  Archive restriction to a total of 20 levels for performance reasons.

- **Maximum compression rate**

  ```
  ArchiveMaxRatio 150
  ```

  Archive restriction to a compression rate of 150, for performance reasons.

- **Maximum of files which should be scannend**

  ```
  ArchiveMaxCount 0
  ```

  Limitation of the amount of files which should be scanned. Usually this is not necessary.

- **Notification level**

  ```
  SuppressNotificationBelow scanner warning
  ```

  Sends email notifications for the component “scanner” in case of an event “warning” and higher. This is recommended for an adequate notification.

- **Define the log file**

  ```
  LogFile /var/log/avguard.log
  ```

  Defines the log files of the OnAccess scanner. This is the default path.

- **Detection of undesired software**

  ```
  DetectPrefixes adspy=yes appl=no bdc=yes dial=yes game=no
  hiddenext=yes joke=no pck=no phish=yes spr=no
  ```

  Offers a protection against undesired Software like e.g. hidden file extensions, phishing, dial up programs, backdoor programs and undesired advertisement pop-ups.

The detection can also be configured by using the following list:

ADSPY
Software that displays advertising pop-ups or software, that very often, without the user‘s consent, sends user specific data to third parties and might therefore be unwanted.

APPL
The term APPL/ denotes an application of dubious origin or which might be hazardous to use.

BDC
Is the control software for backdoors. Control software for backdoors is usually harmless.

DIAL
A Dial-Up program for connections that charge a fee. Its use might lead to huge costs for the user.

GAME
Applies to games that usually cause no harm to your computer.

HEUR-DBLEXT
The file has an executable file extension, but hides it behind a harmless one.

JOKE
A harmless joke program is present as a file.

PCK
A file has been compressed with an unusual runtime compression tool. Please make sure that this file comes from a trustworthy source.

PHISH
Fake emails which are supposed to prompt the user to reveal confidential information such as user accounts, passwords or online-banking data on certain websites.

SPR
Software that may be able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behavior and might therefore be unwanted.

`HeuristicsLevel 2`
Activates the heuristic on medium level
A good balance between detection and early detection which prevents a lot of possible false positives

`HeuristicsMacro yes`
Activates the detection of possible macro viruses in office documents
We recommend the scan of office documents for an optimum of security.

4. Additional configuration options

4.1. No Real Time Protection

You can use only the command line scanner without real time protection by setting the parameter ‚OndemandMgmt yes' in the */etc/avguard.conf*. In that case Dazuko or DazukoFS don't have to be loaded.

4.2. Heavy Load in the System

Depending on the workload you can choose a value between 3 and 20 in the parameter NumDaemons to increase the performance. The settings chosen here should be reflected in the ratio of demand and the available memory.

4.3. Exception of Directories

In general, exceptions should be set at the database directories since those are not scanned correctly due to their internal structure. In addition, they can cause a huge loss in performance.
The exception can be set with the „ExcludePath" parameter.
Example:

/etc/avira/avguard.conf

```
ExcludePath /dbdir
```

5. Particularities - NSS Volumes

The NSS starts very late using e.g. SLES. This causes a malfunction of the already mounted DafukoFS.

Therefore, it is necessary to adjust the run level, so that the concerned shares are mounted after the start of the NSS with DazukoFS. You find more detailed information about the adjustment of the start order in the documentation of the operating system.

6. Command Line Scanner - avscan

The avscan binary offers the OnDemand scan mode and can be activated at /usr/lib/AntiVir/avscan with the user-defined parameters.

The following activation is similar to the above described guard configuration. The parameters can be deduced accordingly. The scan is executed in the /home directory.

The parameter –s stands for a recursive scan in subdirectories. In order to execute the scan automatically without user interaction, the parameter `–batch` can be used. Detections are moved automatically into the quarantine:

```
$ avscan --scan-in-archive=yes --scan-in-mbox=yes --archive-
max-size=0 --archive-max-recursion=0 --archive-max-ratio=0
--scan-mode=all --heur-macro=yes --heur-level=2 --alert-
action=quarantine --quarantine-dir=/home/quarantine -s --batch
/home
```

This can also be executed automatically by using a cron job. We recommend to create the activation in the form of a shell script and to activate it accordingly via cronjob – e.g. once a week, for instance on Saturday at twelve o'clock:

```
00    12    *     *     6     root /usr/local/bin/virenscan.sh
```

7. Update Configuration

In order to keep your Antivirus installation up-to-date, two kinds of updates should be set during the installation:

- Scanner update (only scanner & engine & VDF)
- Product update (Guard program files)

After the installation the settings for the update can be found in the following file:

/etc/cron.d/avira_updater

```
00 */2 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
15 12 * * Tue root /usr/lib/AntiVir/avupdate --product=Guard
```

7.1. Reasonable Values for an Update

Depending on the target group we recommend our customers to perform an update at least 2 or 3 times a day.

7.2. Large Enterprises

Example: hourly update

/etc/cron.d/avira_updater

```
* */1 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

7.3. Small Business

Example: 3 hour interval

/etc/cron.d/avira_updater

```
* */3 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

7.4. Customers with Narrow Strip Connections (modem/ISDN)

Example: 8 hour interval

/etc/cron.d/avira_updater

```
* */8 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

7.5. Internet Service Providers (ISPs)

For internet service providers it is recommended to download the current signatures more frequently, e.g. every 15 minutes. This ensures that you always promptly use the latest signatures.

/etc/cron.d/avira_updater

```
*/15 * * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

7.6. Signature Update

Furthermore, you have the possibility to execute only an engine and VDF update. The guard product files and the central scanner service (SAVAPI) are not updated.

This could be generally very interesting for you if program updates are regarded as particularly sensitive. It will give you the option to perform an audit initially on a separate test system before using the new version productively.

The command has to be entered as follows:

```
$ /usr/lib/AntiVir/avupdate --product=Signatures
```

Issued Q4-2011

AVIRA

live free.™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile +49 7542-500 3000
www.avira.com