avast business

Avast Antivirus for Linux Technical Documentation

AVAST LINUX TEAM, LINUX-AV@AVAST.COM
FRIDAY 12TH JULY, 2019

Overview

The Avast Antivirus for Linux products include the following components which are distributed as standard software packages – DEB for Debian (Ubuntu) systems and RPM for RedHat systems. Software repositories are also provided so that all of the standard system management tools can be used to keep the Avast programs up to date.

Packages

Avast

The avast package provides the core scanner service (avast) and a command line scan utility (scan). Additionally it contains a command line license utility (avastlic). The package allows for on demand scanning and mail server integration using AMaViS as described in section 6.

The avast package is required by the avast-fss packages.

Avast-fss

The *avast-fss* package provides a fanotify based ”on write” file system shield designed for file server usage. The typical target field for avast-fss are SMB/NFS file servers.

Business products

The Avast components are available as the following business products:

Avast Security Suite for Linux

License for all packages.

Contents

Overview 1

Installation 2

Operation 2

Licensing 3

Virus definitions updates 3

AMaViS integration 4

Appendices 4

- Scan manual page 4
- Avast manual page 5
- Avast-fss manual page 6
- Avastlic manual page 7
- Avast public encryption key 8

Installation

The Avast Linux server product is installed in two steps:

1. Add the Avast repository to the system repositories.
2. Get the desired packages from the repository.

Debian/Ubuntu

1. Add the Avast repository to the system repositories

   Debian(pre-9 stretch)/Ubuntu(pre-18.04 Bionic Beaver):
   # echo "deb http://deb.avast.com/lin/repo debian release" \
   >> /etc/apt/sources.list

   Ubuntu 18.04 Bionic Beaver:
   # echo "deb http://deb.avast.com/lin/repo ubuntu-bionic release" \
   >> /etc/apt/sources.list

   Debian 9 stretch:
   # echo "deb http://deb.avast.com/lin/repo debian-stretch release" \
   >> /etc/apt/sources.list

   Debian 10 buster:
   # echo "deb http://deb.avast.com/lin/repo debian-buster release" \
   >> /etc/apt/sources.list

2. Install Avast public key and update package manager state
   # apt-key add /path/to/avast.gpg
   # apt-get update
3. Install the avast package and optionally the avast-fss package.
   # apt-get install avast
   # apt-get install avast-fss

RHEL/CentOS

1. Add the Avast repository to the system repositories:
   # echo '[avast]
   name=Avast
   baseurl=http://rpm.avast.com/lin/repo/dists/rhel/release enabled=1
   gpgcheck=1' > /etc/yum.repos.d/avast.repo
   # rpm --import /path/to/avast.gpg
2. Install the avast package and optionally the avast-fss[1] package.
   # yum install avast
   # yum install avast-fss

The current virus definitions database (VPS) is downloaded during the installation of the avast package, so the installation may take some time.

The Avast GPG public key referenced as avast.gpg can be found in appendix E.

Operation

All Avast packages provide conventional init scripts for starting/stopping the services. For example starting the core Avast service is done by running

/etc/init.d/avast start

and stopping the service is done by running

/etc/init.d/avast stop

All Avast services use the system logger (syslog) to create log files and the location is dependent on the host system. The most common log file paths are

/var/log/messages and /var/log/syslog.

Licensing

Access to the program repositories are not restricted in any way. The latest packages are always available, but require a license file to run the components. The license for the products comes in the form of a file named license.avastlic. When you have the license file, copy it into the /etc/avast directory:

cp /path/to/license.avastlic /etc/avast

In case you have been provided with an activation code, use the avastlic(1) tool to download the license. Please note that for some codes this can only be done limited number of times. Also, some activation codes require a customer information to be entered and as such the tool is by default interactive when the activation code mandates this information:

$ avastlic -f new_license_file_path -c avast_activation_code
$ sudo cp new_license_file_path /etc/avast/license.avastlic

In case the downloaded license is valid for multiple machines, it is recommended to download the license
once and then distribute the license file to all the other machines.renced as avast.gpg can be found in appendix E.

Virus definitions updates

Regularly updating the virus definitions database (VPS) is necessary to keep your antivirus protection up to date. Avast antivirus provides a shell script which checks for, downloads and installs the latest VPS. The update script is installed by default and executed every hour as a cron job.

The default Avast crontab entry is:

0 * * * * /var/lib/avast/Setup/avast.vpsupdate

Avast uses incremental updates, so the average update data size is less than 0.5MB.

Local virus definitions mirrors

It is possible to use a local, mirrored, VPS repository. This is useful when you are running several Avast installations on your local network.

To set up a local VPS mirror, all you need is a local HTTP server that can serve a copy of the official public repository. To get your local repository copy, use the following command[2]:

```
$ wget -r -N -e robots=off -nH --cut-dirs=2 \
"http://linux-av.u.avcdn.net/linux-av/avast/x86_64/vps9/"
```

To change the VPS repository URL that Avast uses for VPS updates edit the

/etc/avast/vps.conf configuration file.

Security considerations

The update files are signed by Avast, and the application verifies the signature before applying an update.

AMaViS integration

AMaViS is an interface between mailer (MTA) and content checkers, which is already prepared for integration with mail scanners. This section describes how to integrate avast into AMaViS.

Integration of Avast into AMaViS includes AMaViS configuration updates and enabling access to emails going through AMaViS for Avast to scan. This can be

divided into three steps:

1. Integrating Avast antivirus

   Open the AMaViS configuration file (e.g. /etc/amavis/conf.d/50-user) and insert the following lines into the file:

   ```
   @av_scanners = (
   ### http://www.avast.com
   ['Avast', '/usr/bin/scan', '{}', [0], [1], qr/\t(.+)/m]
   );
   ```

2. Enabling Virus Scanning

   Then open the AMaViS content filter configuration file (e.g. /etc/amavis/conf.d/15-content_ filter_mode) and enable antivirus checking mode by uncommenting the ’bypass virus checks’ lines.

3. Updating Access Permissions

   Finally enable the Avast scan service to scan emails going through AMaViS:

   ```
   # usermod -G amavis -a avast
   ```

[2] *Replace x86 64 with i386 for 32b systems*

Appendices

Scan manual page

scan - Avast command line scan utility

Synopsis

scan [-s SOCKET] [-e PATH] [-abfipux] [PATH]...
scan [-s SOCKET] [-a] -U [URL]...
scan [-s SOCKET] -V
scan -h | -v

Description

Scan is the basic command line scanner that comes with Avast for OS X. It searches the given PATH(s) for infected files and reports such files to the standard output. If no PATH is given, the scan paths are read from the standard input, line by line.

The scan tool is a client that connects to the Avast scan service, it cannot work separately, without a running scan service.

Options

-h Print short usage info and exit.

-v Print program version and exit.

-V Print the virus definitions (VPS) version and exit. The VPS version is retrieved from the scan service.

-U Check URLs. Checks whether an URL is malicius.
Note: the URL is checked against a blacklist, no network request to the given URL is done.

-s SOCKET
Use SOCKET to connect to the scan service. The default scan socket path is "/Library/Application Support/Avast/run/scan.sock".

-e PATH
Exclude PATH from the scan. Use this option multiple times when more than one exclude path is required.

-a Print all scanned files/URLs, not just infected.

-b Report decompression bombs as infections. When set, files suspected of being decompression bombs are reported as infected, not as errors.

-f Scan full files. When set, the entire file contents are scanned, not just the relevant file parts.

-i Print verbose infection info. When set, verbose info about all infections found in the scanned file is printed.

-l LEVEL
Set heuristics level to LEVEL (0-100).

-p Print archive content. When set, the files in an archive are listed separately, with the scan status for each shown.

-u Report potentially unwanted programs (PUP). When set, PUP files are reported as infected.

-x Do not extract archives. When set, compressed files are not extracted during scan.

Output Format

Every detected malicious file is reported on a separate line in the format:

PATH INFECTION
Where PATH and INFECTION are separated by a TAB character. If all files are printed using the -a option, then the clean files have a "[OK]" string as the infection name and files that could not be scanned (insufficient permissions, corrupted archives, ...) have an "[ERROR]" string as the infection name. Files, that were excluded from the scan using the -e option have a "[EXCLUDED]" string as the infection name.

If the -p option is set, PATH contains the archive path delimited by a "|>" delimiter in case of an archive.

Access Rights

It is the scan service that is accessing the files being scanned, not the scan utility itself, therefore the scan service must have access rights to the scanned files. Connections to the scan service may be restricted to clients with the same UID/GID if enabled in the scan service configuration.

Exit Status

The exit status is 0 if no infected files are found and 1 otherwise. If an error occurred, the exit status is 2. Infected status takes precedence over error status, thus a scan where some file could not be scanned and some infection was found returns 1.

Avast manual page

avast - Avast antivirus scanner

Synopsis

avast [OPTIONS]

Description

avast is an antivirus scan service for OS X and Linux. Clients (shields, command line scan tool, ...) connect to the service's UNIX socket and perform scan requests and receive scan results.

Options

-h Print short usage info and exit.

-v Print the program version and exit.

-d DIR Verify that DIR is a valid data directory and contains a valid VPS. If the exit code is nonzero, than the VPS is missing or invalid. The check may generate some data files in the VPS directory if they are missing but can be generated from the corresponding "source" files.

-c FILE
Set configuration file path to FILE. The default configuration file is /etc/avast/avast.conf.

-n Do not daemonize.

Configuration

The configuration file format is INI file format, i.e. it consists of KEYWORD = VALUE entries, each on a separate line. Lines beginning with ';' are treated as comments and are ignored. Keys may be grouped into arbitrarily named sections. The section name appears on a line by itself, in square brackets ([and]).

The following example is an avast configuration file with explicitly defined default options:

```
; Avast configuration file
RUN_DIR = "/var/run/avast"
TEMP_DIR = "/tmp"
DATA_DIR = "/var/lib/avast"
SOCKET = "/var/run/avast/scan.sock"
LICENSE = "/etc/avast/license.avastlic"
WHITELIST = "/etc/avast/whitelist"
SUBMIT = "/var/lib/avast/Setup/submit"
[OPTIONS]
CREDENTIALS = 0
STATISTICS = 1
HEURISTICS = 1
STREAMING_UPDATES = 1
```

The configuration file is re-read on HUP signal by the program, but only the entries in the Options section are reloaded, changes to the global parameters are ignored.

Global parameters

RUN_DIR
Run directory. The PID file is stored here.

TEMP_DIR
Temporary directory. The program temporary files are stored here.

DATA_DIR
Data directory. Contains the virus definitions database and various other data files used by avast.

SOCKET
Path to the UNIX socket used by the clients to connect to the scan service. The socket is created by avast at service start.

LICENSE
Path to the license file.

WHITELIST
Path to the whitelist file. The whitelist file contains sha256 hashes of files, that shall not be reported as infections even though detected by the scan engine. The file format is one sha256 hash in text mode per line. Hash mark (#) prefixed comments can be used in the file.

SUBMIT
Path to the submit utility. If enabled (see the Options section), the submit utility creates and sends reports about infected and suspicious files to the avast virus lab.

Options

CREDENTIALS
If enabled, avast performs a UNIX socket credentials check, whenever a new client is

connecting. If the client's effective UID does not match the effective UID of the avast process or the client's effective GID does not match the avast effective GID or any avast supplementary group GID, the connection is refused.

STATISTICS
If enabled, avast creates statistics submits about detected malicious files.

HEURISTICS
If enabled, avast creates heuristics submits about suspicious files detected during the scan.

STREAMING_UPDATES
If enabled, the scan service establishes a permanent network connection to the avast cloud and retrieves virus definitions updates instantly as they are released. Streaming updates are an addition to the regular virus database updates, they

do not replace them (you always get all the streamed updates in the next regular virus definitions database update).

SEE ALSO
scan(1), avast-protocol(5)

Avast-fss manual page

avast-fss - Avast file server shield

Synopsis

avast-fss [OPTIONS]

Description

avast-fss, a part of Avast antivirus for Linux suite, provides real-time scanning of files written to any of the monitored mountpoints. avast-fss is based on the fanotify access notification system available on Linux kernels 2.6.37+.

Options

-h Print short usage info and exit.

-v Print the program version and exit.

-c FILE - Set configuration file path to FILE. The default configuration file is /etc/avast/fss.conf.

-n Do not daemonize.

Configuration

The configuration file format is INI file format as described in the avast(1) manual page.

The configuration consists of two parts - the global configuration options and the monitoring configuration. The sample configuration below shows all available global configuration options and their default values followed by some examples of monitoring (and monitoring exclude) entries.

```
; Avast fileserver shield configuration file
RUN_DIR = "/var/run/avast"
SOCKET = "/var/run/avast/scan.sock"
LOG_FILE = "/var/log/avast/fss.log"
CHEST = "/var/lib/avast/chest"
SCANNERS = 4
UNLIMITED_QUEUE = 0


[MONITORS]
SCAN = "/some/mountpoint/to/monitor"
SCAN = "/another/mountpoint/to/monitor"
EXCL = "/path/to/exclude/from/scan"
```

Global parameters

RUN_DIR
Run directory. The PID file is stored here.

SOCKET
Path to the avast service UNIX socket.

LOG_FILE
Path to the virus log file.

CHEST
Path to the chest directory. The chest directory is where the detected malicious files are moved. If the chest directory is located on a monitored mountpoint, it is automatically added to the excluded paths on startup.

SCANNERS
Number of parallel running scans. Set this option to the number of CPU cores to get the best performance.

UNLIMITED_QUEUE
If set to 1, avast-fss disables the limit on the fanotify event queue size. For more info, see FAN_UNLIMITED_QUEUE in fanotify_init(2).

Monitors
SCAN
A mountpoint (path) that shall be monitored by avast-fss. If the given path is not a system mountpoint, it is automatically converted to the corresponding mountpoint.

EXCL
A path to be excluded from monitoring.

SEE ALSO
avast(1), fanotify(7)

Avastlic manual page

avastlic - obtains license for Avast Antivirus for Linux

Synopsis

avastlic -f new_license_file_path -c
avast_activation_code [-n]
avastlic -h

Description

The avastlic(1) command can be used to convert Avast Antivirus activation code into a license file. Please note that for some codes this can only be done limited number of times. Also, some activation codes require a customer information to be entered and as such the tool is by default interactive when the activation code mandates this information.

After downloading a license file with avastlic(1), install it by copying it to /etc/avast/license. avastlic. In case the downloaded license is valid for multiple machines, it is recommended to download the license once and then distribute the license file to all the other machines.

Options

-f File path to store the obtained license into.

-c Activation code valid for Avast Antivirus for Linux

-n Non-interactive mode. If the activation code requires customer information, the activation will fail.

-h, --help
Print help.

SEE ALSO
avast(1), scan(1), avast-protocol(5)

Avast public encryption key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.12 (GNU/Linux)

mQENBFMoeIMBCACnCOmAfky/MIa7p2VpDrPtCWdjsMQm+Frf9fVRcgNvZYzexrGv
Qun7tDgCELyAYmElYg/45YeqRT+l5fxpVwG0Unz7jYnHWxt16ojZL2eKI85QDkox
2UUdEkYq8ruECirpg+lUenrO0UQpZKqgx+lYgYQfWrh0cbrKziO0/GCEGpwnI0Iu
lh283mD/AvxY3DyvBjNFk1en1zFFJV5Df4ppZF1vWkIVbv23VDXyooLYNSXk1yJ/
zXLF50p3ex4tdlkGV6ce64iShlO2yfp/36vCyBVsCL8Y4dEeSQZu+4bPkVmyUV75
QmtIb0EDOqdC8MElmGd/s2uoJP1HFl1SUKKvABEBAAG0OkF2YXN0IFNvZnR3YXJl
IHMuci5vLiAoUmVsZWFzZSBFbmdpbmVlcmluZykgPHJlQGF2YXN0LmNvbT6JATgE
EwECACIFAlMoeIMCGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEJHuE/BX
Ty17OhAIAKA/vGSTWvT1Bm049fwNudWXxBc3l97meqa0DVTv2TzCOiK3W5w/CKUQ
RaTXYHpak6lbRMeRu8kShvlKBJ15CsoKUSz0zTgrwxmDhiYBcsafh0R81+51jEll
YxAZfBkKZtI4RJxXFpbOVVe9AeOnMgTdFreNK/E0tjZQStNUKl1W7kDPV3W3eVbY
JAdUbBHBvqvkBHZ90B0kgeOofHZ2z1GQCCc1ClxSw2n0WDFlQ96cfSL8YeHb1bbF
P+hMW1V1L6lgN7VdpfhsOdGhzPb9VCU4K/pGzSSNeg1ksVCH2bm+7Y8AoX2BSVDT
5UbYbrt9AdDES9nuKSmFrqgbtdxZJO65AQ0EUyh4gwElANI4a5lOnaA/mRySIIlm
JMovZJzH5muO0ao7D3SiWtyT7DSPo6LzO3eLnC0AjZ+dT14kVKiekRNMD/3cSPNP
2ulbeTe00RbmaCz30w+vWWdt2IWKGB8whvkUh/4dzbY49FHek0+WkaLJRD1UlUE5
13ICmU6m7xeMv64tN3cWwuEYjQoJLRQezR1u0GU+0MSDv3J813WwZbxU5XYX71hO
2G/CD9utu4eUl0MpPBv5x9e1sPjUET6e0xS7RmRzk4mxBAiUtIT2RcOELghPj1q7
oNBuaUkeHhx5aebokJKxzekto8fpjRo7OGlVe/QlZxL1UD+QxyVPfVNpVyOUHvYI
qzsAEQEAAYkBHwQYAQIACQUCUyh4gwIbDAAKCRCR7hPwV08te0RCB/9vF538ooRD
bgRBBN5mviKxuxFnrEQYsPpZvmEsHvS6RSQfPvmVF3z4HUoKHWFsqRbhaJCRVWbm
fl8X8DOezAVR734MYaicj+NzVdKAKWu+a5TJ5XxVG2mSY+a0PK3FkF4cSH2fgmxq
q/NiYFVY2SZpwEOg+zkYF8m1+DoxSpeJ7wapPcFhgIt5YS6Bego6AM1Ork2yTXY7
95ZMFyFjT9XJJUo9BG4NMnzVxsgMhJ6g1zGKtsoVrPgxmyJ5KHA+Hr5BvkESuXQw
mQp5EeiKUqxAWe7wbk59oSKUNYAJen/X3jCCYaXqN1vEX5E6kcZO2O6e2II32ecP
r4XP+TMQpz3L
=nuBs
-----END PGP PUBLIC KEY BLOCK-----

About Avast Business

Avast delivers all-in-one cybersecurity solutions for today's modern workplace, providing total peace of mind. Avast provides integrated, 100% cloud-based endpoint and network security solutions for businesses and IT service providers. Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. Our easy-to-deploy cloud security solutions are built to offer maximum protection businesses can count on. For more information about our cloud-based cybersecurity solutions, visit **www.avast.com/business**.