

fsavd

<support@F-Secure.com>

Juha AuteroSami Mäkinen-Okubo2002-10-26

Name

fsavd — F-Secure Anti-Virus for Linux daemon

Synopsis

fsavd [*options*]

DESCRIPTION

fsavd is a scanning daemon for F-Secure Anti-Virus for Linux. In the startup it reads the configuration file (the default configuration file or the file specified in the command line) and starts to listen connections to the UNIX domain socket specified in the configuration file. By default, **fsavd** forks itself into the background.

Normally fsavd is launched automatically by the fsav client if fsavd is not running. If fsavd is launched by the fsav client, fsavd terminates automatically after 30 seconds of idle time, i.e. no client has connected to fsavd during the time.

You can also start **fsavd** using the `<install directory>/etc/fsavd` startup script if you want fsavd to stay loaded in the memory. It is recommended that you run **fsavd** as a non-privileged user like [fsav]. The script is suitable to be installed under the `init.d`-directory.

The fsavd uses F-Secure File Management Library which is installed as a shared library under the `<install dir>/lib/libfm.so`. To run fsavd straight from the command-line the library must be available for the dynamic linker before fsavd can be started. This can be done by setting the `LD_LIBRARY_PATH` to point to the library directory, e.g in bash(1):

```
$ export LD_LIBRARY_PATH=<install dir>/lib
$ fsavd
```

OPTIONS

fsavd reads option values from the configuration file and from command-line. If the configuration file is not given from the command-line, `$HOME/.fsav.conf` or `/etc/fsav.conf` is used instead. If neither of configuration files exist, the default values are used. The options given from the command-line override the configuration file options.

fsav and fsavd should use the same configuration file. If fsav uses different configuration file than fsavd, the running fsavd does not use the values specified in the configuration file that fsav uses, i.e. to change configuration file settings for fsavd fsavd has to be restarted.

The default options or configuration file options can be overridden from the command-line with the following command-line options:

`--configfile=configurationfile`

Use the configuration file *configurationfile*.

`--databasedirectory=path`

Read virus description databases from the directory *path*. The default is ". ".

`--enginedirectory=path`

Load scan engines from the directory *path*. The default is ". ".

`--socketname=path`

Use the socket specified in the path. The default is "/tmp/.fsav-<UID>".

`--standalone`

Start in the stand-alone mode, i.e. auto-terminate after a period of idle time.

`--nodaemon`

Do not fork program into the background.

`--help`

Show command line options and exit.

`--version`

Show F-Secure Anti-Virus for Linux version and dates of signature files, and exit.

LOGGING

fsavd logs scan failures, infected and suspected files to the fsavd's log file defined with the *logfile* configuration file option (see fsav.conf(5) for more information). fsavd writes errors during start-up to standard error stream. After successful start-up log entries are written to a log file. Error messages listed in errors section are also logged in addition to the following activity log entries:

Failed to scan file <file path>: <error message> [<scan engine>]

Explanation: The scan engine reports it failed to scan the file. The error message contains the reason for the failure.

Failed to scan file <file path>: Time limit exceeded.

Explanation: fsavd reports that the file scan failed because the scan time limit is exceeded.

Failed to scan file <file path>: Scan aborted.

Explanation: fsavd reports that the file scan failed because the scan was aborted. The scan is aborted if the client disconnects.

File <file path> disinfected.

Explanation: fsavd reports that one of the scan engines disinfected the file successfully.

File <file path> disinfect failed.

Explanation: fsavd reports that all the scan engines failed to disinfect the file.

File <file path> infected: <infection name> [<scan engine>]

Explanation: The scan engine reports that the file was found infected.

File <file path> contains suspected infection: <infection name> [<scan engine>]

Explanation: The scan engine reports that the file contains a suspected infection.

WARNINGS

Unknown action '*<user given value>*' in configuration file *<file path>* line *<line number>*

Explanation: The *action* in the configuration file has an incorrect value.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and set the *action* field to one of the following: *disinfect*, *rename* or *delete*. The user has to restart fsavd to take values in effect.

Configuration file *<file path>* has invalid syntax at line *<line number>*

Explanation: The configuration file parsing has failed because of invalid syntax.

Resolution: fsavd tries to proceed and probably encounter some other error later. The user has to edit the configuration file and restart fsavd.

Illegal archive scanning value '*<user given value>*' in configuration file *<file path>* line *<line number>*

Explanation: The *archivescanning* field in the configuration file has an incorrect value.

Resolution: fsavd tries to proceed. The user has to edit configuration file and set the *archivescanning* field to one of the following: *1*, *0*, *on*, *off*, *yes*, or *no*. The user has to restart fsavd to take values in effect.

Illegal MIME scanning value '*<user given value>*' in configuration file *<file path>* line *<line number>*

Explanation: The *mimescanning* field in the configuration file has an incorrect value.

Resolution: fsavd tries to proceed. The user has to edit configuration file and set the *mimescanning* field to one of the following: *1*, *0*, *on*, *off*, *yes*, or *no*. The user has to restart fsavd to take values in effect.

Illegal scan executables value '*<user given value>*' in configuration file *<file path>* line *<line number>*

Explanation: The *scanexecutables* field in the configuration file has an incorrect value.

Resolution: The user has to edit configuration file and set the *scanexecutables* field to one of the following: *1, 0, on, off, yes, or no*. The user has to restart fsav to take values in effect.

Scan extensions list is too long in configuration file <file path> line <line number>, list is truncated.

Explanation: The *extensions* field in the configuration file is more than 4096 bytes long.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and try again.

Scan timeout value '<user given value>' is not valid in configuration file <file path> line <line number>

Explanation: The *scantimeout* field in the configuration file is not a valid number.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and restart fsavd.

Scan timeout value '<user given value>' is out of range in configuration file <file path> line <line number>

Explanation: The *timeout* field in the configuration file is less than zero or more than LONG_MAX.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and restart fsavd.

Maximum nested archives value '<user given value>' is not valid in configuration file <file path> line <line number>

Explanation: The *maxnestedarchives* field in the configuration file is not a number.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and restart fsavd.

Maximum nested archives value '<user given value>' is out of range in configuration file <file path> line <line number>

Explanation: The *maxnestedarchives* field in the configuration file is less than zero or more than LONG_MAX.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and restart fsavd.

Maximum scan engine instances value '<user given value>' is not valid in configuration file <file path> line <line number>

Explanation: The *engineinstancemax* field in the configuration file is not a number.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and try again.

Maximum scan engine instances value '<user given value>' is out of range in configuration file <file path> line <line number>

Explanation: The *engineinstancemax* field in the configuration file is less than zero or more than LONG_MAX.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and try again.

Unknown option '<user given option name>' in configuration file <file path> line <line number>

Explanation: The configuration file contains an unknown option name.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and restart fsavd.

Unknown syslog facility '<user given value>' in configuration file <file path> line <line number>

Explanation: The *syslogfacility* field in the configuration file has an incorrect value.

Resolution: fsavd tries to proceed. The user has to edit configuration file and set the *syslogfacility* field to one of the facility names found in syslog(3) manual page. The user has to restart fsavd to take values in effect.

<engine name> scan engine seems to be dead.

Explanation: The scan engine <engine name> has died. Either the timeout occurred during the file scan or the scan engine process has died unexpectedly.

Resolution: fsavd has noticed the scan engine has died. fsavd tries to restart the scan engine. If the scan engine was scanning a file, the file is reported to be failed to scan.

Database file <file path> not needed and should be deleted.

Explanation: The scan engine reports that the database directory contains a deprecated database file.

Resolution: The message is only informational. The user may delete the file in path <file path>.

Database file <file path> is missing.

Explanation: The scan engine reports that the database file <file path> is missing from the database directory.

Resolution: The scan engine fails to start. fsavd will try to restart the scan engine. The user needs to perform database update and possibly restart fsavd if fsavd fails to start the scan engine automatically.

Database file <file path> is not a valid database.

Explanation: The scan engine reports that the database file <file path> is not a valid database file in the database directory.

Resolution: The scan engine fails to start. fsavd tries to restart the scan engine. The user needs to perform database update and possibly restart fsavd if fsavd fails to start the scan engine automatically.

Database file <file path> is not a database file.

Explanation: The scan engine reports that the database file <file path> is not a valid database file in the database directory.

Resolution: The scan engine fails to start. fsavd tries to restart the scan engine. The user needs to perform database update and possibly restart fsavd if fsavd fails to start scan engine automatically.

Database file *<file path>* is corrupted.

Explanation: The scan engine reports that the database file *<file path>* is not a valid database file in the database directory.

Resolution: The scan engine fails to start. fsavd tries to restart the scan engine. The user needs to perform database update and possibly restart fsavd if fsavd fails to start the scan engine automatically.

Database file *<file path>* has wrong database version.

Explanation: The scan engine reports that the database file *<file path>* has an incorrect version.

Resolution: The scan engine fails to start. fsavd tries to restart the scan engine. The user needs to perform database update and possibly restart fsavd if fsavd fails to start the scan engine automatically.

***<engine name>* scan engine initialization time limit exceeded, going for shutdown.**

Explanation: The scan engine has exceeded its initialization time limit (300 seconds). The reason may be a high system load and thus the scan engine processes do not get enough processing time to load the databases. Furthermore, the hardware failure may cause the scan engine to hang while reading the databases.

Resolution: fsavd shuts down the scan engine process and tries to restart the scan engine. If problem still occurs, the user may try to update databases or scan engine to resolve the problem. If the problem persists the user needs to contact F-Secure support.

***<engine name>* scan engine inactive for too long, going for shutdown.**

Explanation: The scan engine is not responding to the keep-alive messages and it has not reported scan nor initialization statuses for a limited time period (300 seconds). The problem may be in a file which the scan engine is scanning. If the user can recognize the source as a problematic file, the user should make a bug report and send a file sample to F-Secure.

Resolution: fsavd shuts down the scan engine process and restarts the scan engine.

Could not open logfile <file path>: <OS error message>

Explanation: fsavd failed to open the logfile <file path> for logging.

Resolution: fsavd writes logs to default logfile (stderr). The user may reconfigure the logfile location and restart fsavd.

Cannot change working directory to '<file path>'.

Explanation: fsavd failed change working directory database directory.

Resolution: fsavd tries to continue using the current directory as working directory.

ERRORS

Failed to open scan engine shared library.

Explanation: fsavd cannot find required scan engine shared library files which are normally found from <install directory>/lib.

Resolution: fsavd exits with error status. Installation or engine directory in configuration file maybe incorrect or --enginedirectory command-line option has incorrect path.

Failed to load required symbol from scan engine library.

Explanation: fsavd finds required scan engine shared library files but fails to load correct library calls from the library.

Resolution: fsavd exits with error status. Scan engine shared libraries are corrupted. Product needs to be re-installed.

Options parsing failed.

Explanation: The user has given an unknown option or an option value from the command-line.

Resolution: fsavd exits with error status. The user has to correct the command-line parameters and start fsavd again.

Database directory '*<directory path>*' is not valid in configuration file at line *<line number>*: *<OS error message>*

Explanation: The user has entered a database directory path which either does not exist, is not accessible or is too long from the configuration file.

Resolution: fsavd exits with error status. The user has to correct the path and start fsavd again.

Database directory '*<directory path>*' is not valid: *<OS error message>*

Explanation: The user has entered a database directory path which either does not exist, is not accessible or is too long from the command-line.

Resolution: fsavd exits with error status. The user has to correct the path and start fsavd again.

Database update directory '*<directory path>*' is not valid in configuration file at line *<line number>*: *<OS error message>*

Explanation: The user has entered a database update directory path which either does not exist, is not accessible or is too long from the configuration file.

Resolution: The user has to correct the path and start fsavd again.

Scan engine directory '*<directory path>*' is not valid in configuration file at line *<line number>*: *<OS error message>*

Explanation: The user has entered a scan engine directory path which either does not exist, is not accessible or is too long from the configuration file.

Resolution: fsavd exits with error status. The user has to correct the path and start the fsavd again.

Scan engine directory '*<directory path>*' is not valid: *<OS error message>*

Explanation: The user has entered a scan engine directory path which either does not exist, is not accessible or is too long from the command-line.

Resolution: fsavd exits with error status. The user has to correct the path and start the fsavd again.

Could not open configuration file *<file path>*: *<OS error message>*

Explanation: The configuration file path given from the command-line, the file does not exist or it is not accessible.

Resolution: fsavd tries to proceed and probably encounters some other error later. The user has to create the configuration file to the default path or give the correct path to an accessible configuration file and restart fsavd.

Access to database index file '*<file path>*' failed: *<OS error message>*

Explanation: The database directory path (set in the configuration file or from the command-line) is not correct and the daemon cannot find the `dbindex.cpt` file.

Resolution: fsavd exits with error status. The user has to give the correct database path and start fsavd again.

stat for database index file failed: *<path to dbindex.cpt>*

Explanation: The database directory path (set in the configuration file or from the command-line) is not correct and fsavd cannot find the `dbindex.cpt` file.

Resolution: fsavd exits with error status. The user has to give the correct database path and start fsavd again.

accept failed because run out of memory.

Explanation: The `accept(2)` has failed because system ran out of the memory.

Resolution: fsavd exits with error status. The user has to free some memory and start fsavd again.

FILES

`/etc/fsav.conf`

The default configuration file for F-Secure Anti-Virus for Linux

`$HOME/.fsav.conf`

User specific configuration file for F-Secure Anti-Virus for Linux

`<install directory>/etc/fsav`

Startup file for F-Secure Anti-Virus for Linux

`<install directory>/databases`

Directory for Anti-Virus signature database files.

`<install directory>/lib`

Directory for Anti-Virus scan engine and F-Secure Anti-Virus for Linux shared library files.

EXAMPLES

The following examples assume the `LD_LIBRARY_PATH` is set correctly or the `libfm.so` file is installed to the system library directory. To set `LD_LIBRARY_PATH` in `bash(1)` use the following command:

```
$ export LD_LIBRARY_PATH=<install dir>/lib
```

Start `fsavd` as a background daemon process using the default configuration file:

```
$ fsavd
```

Start `fsavd` as a foreground process using the default configuration file:

```
$ fsavd --nodaemon
```

Start `fsavd` as a background daemon process using `'fsav-test.conf'` as a configuration file:

```
$ fsavd --configfile=fsav-test.conf
```

Check `fsavd`, scan engine and database versions:

```
$ fsavd --version
```

Bugs

Please refer to 'Known Problems' -section in release notes.

AUTHORS

F-Secure Corporation

Copyright

Copyright (c) 1999-2004 F-Secure Corporation. All Rights Reserved. Portions Copyright (c) 2001-2004 Kaspersky Labs.

SEE ALSO

dbupdate(8), fsav(1), fsav.conf(5) and fsavschedule(8)

For more information, see F-Secure Web Club home page (<http://www.F-Secure.com/anti-virus/webclub/>).