NAME

esets_zmfi − ESETS ZMailer contentfilter module.

SYNOPSIS

esets_zmfi

DESCRIPTION

The **esets_zmfi** is ZMailer's contentfilter, which scans mail filenames read from stdin, requests **esets_daemon** to scan it and responds with the status.

CONFIGURATION FILE OPTIONS

The main ESETS configuration mechanism is assumed to be that using ESETS main configuration file. Note that most principles of this mechanism are described in the esets.cfg(5) manual page while this section contains only additional information related with the list of configuration file options valid for this particular module. Therefore we recommend user to become familiar with the above mentioned documentation prior reading this section.

ESETS MODULE PRIVATE OPTIONS

The **esets_zmfi** has not private options.

ESETS MODULE COMMON OPTIONS

To get detailed description of ESETS module common options, please refer to the section **ESETS MODULE COMMON OPTIONS** of the **esets.cfg(5)** manual page.

ESETS SCANNER COMMON OPTIONS

To get detailed description of ESETS scanner common options, please refer to the section **ESETS SCANNER COMMON OPTIONS** of the **esets.cfg(5)** manual page.

USER SPECIFIC CONFIGURATION

The ESETS system implements possibility to define so called user specific configuration, i.e. relevant configuration parameters specific for e-mail recipient and/or e-mail sender can be defined.

As described in section **USER SPECIFIC CONFIGURATION** of esets.cfg(5) manual page the user specific configuration is created when an appropriate special configuration section created within a special configuration file *path* referenced from this agent section (see main ESETS configuration file) by option **user_config =** *path*.

The header name of user specific section must be in general of the following format,

```
[s_eml|c_eml]
```

where 's_eml' is server's (i.e. recipient's) fully qualified email address or its domain subset, 'c_eml' is client's (i.e. sender's) fully qualified email address or its subset.

Note that it is not mandatory to define both client's and server's parts of the header name. In this case the appropriate part not present within header name will be assumed to be not restricted. The following example shows definition of section with the section header name compound only from the client's e-mail address for which we would like to define special configuration.

```
[|username@domain.com]
av_scan_obj_archives = yes
```

Please, note that thanks to '|' character present at the beginning of section header name, the main ESETS daemon knows that an appropriate email address represents the client's part of the section header name. In case you omit the character '|', the appropriate content of the section header name will be assumed to be its server's part as shown in an example below.

```
[username@domain.com]
av_scan_obj_archives = yes
```

Note also that the section header name can be only domain subset of an appropriate fully qualified email

address as shown in an example below

```
[domain.com]
av_scan_obj_archives = yes
```

or even

```
[org|domain.com]
av_scan_obj_archives = yes
```

The esets_zmfi agent extracts sender and recipient addresses from the ZMailer header of scanned mails automatically.

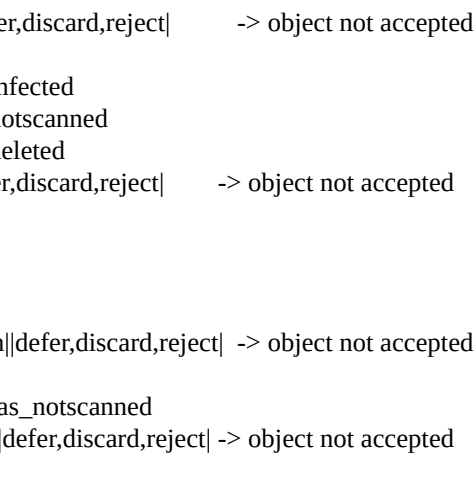
Once fully qualified recipient's and/or sender's email address passed to the daemon, it is compared with section header names found in the special configuration file. The comparison is performed with all section header names consecutively in order as they are written within the file. The configuration appropriate to the first matched section is chosen. If no section header name matches the recipient's/sender's email address passed to the daemon, the configuration appropriate to the agent section from main ESETS configuration file is chosen. The section header name matching algorithm is as follows:

1. If no recipient's address passed to the daemon or no recipient's part of the section header name present, the algorithm returns match for this part of section header name. If fully qualified recipient's address 'rcptname@rcptdomain.com' passed to the daemon, the algorithm compares this address and its parts (i.e. consecutively 'rcptname@rcptdomain.com', 'rcptdomain.com', 'com' is compared) with the recipient's part of the section header name.
2. Similarly if no sender's address passed to the daemon or no sender's part of the section header name present, the algorithm returns match for this part of section header name. If fully qualified sender's address 'sndrname@sndrdomain.com' passed to the daemon, the algorithm compares this address and its parts (i.e. consecutively 'sndrname@sndrdomain.com', 'sndrdomain.com', 'com' is compared) with the sender's part of the section header name.

If both comparison steps described above return match the configuration appropriate to the section header name is chosen. On the other hand if at least one of the steps returns no match, an appropriate section is skipped.

HANDLE OBJECT POLICY

The Handle Object Policy (see figure below) is a mechanism that provides handling of the scanned e-mail messages depending on their scanning status. The mechanism implemented in this module is based on so called action configuration options **action_av**, **action_av_infected**, **action_av_notscanned**, **action_av_deleted**, **action_as**, **action_as_spam** and **action_as_notscanned**. To get description of these configuration options, see esets.cfg(5) manual page.



+------+
object accepted

Every e-mail message processed by this module is first handled with respect to the setting of the configuration option **action_av**. Once the option is set to 'accept' (resp. 'defer', 'discard', 'reject') the object is accepted (resp. deferred, discarded, rejected). If the option is set to 'scan' the object is scanned (resp. also cleaned if requested by configuration option **av_clean_mode**) for virus infiltrations and set of action configuration options **action_av_infected**, **action_av_notscanned** and **action_av_deleted** is taken into account to evaluate further handling of the object. If action 'accept' has been taken as a result of the three above action options the object processed shall be scanned for spam.

Note that the e-mail message is scanned for spam only in case the configuration option **action_as** is set to 'scan'. In this case the action configuration options **action_as_spam** and **action_as_notscanned** is taken into account. If action 'accept' (resp. 'defer', 'discard', 'reject') has been taken as a result of the two above action options the object is accepted for further delivery (resp. the object is deferred, discarded or rejected).

You have probably noticed that each of the action configuration options discussed above accepts a variety of the values whose list can be found in esets.cfg(5) manual page. As also stated there the values listed are handled individually by every ESETS agent module. Thus to be consistent in the following we review the meaning of the values for this ESETS agent module.

accept Accept object on this level of Handle Object Policy, i.e. access to the object is allowed by the particular action configuration option.

scan Scan object for virus infiltrations (resp. for spam) and clean infected objects if requested by configuration option **av_clean_mode**.

defer Return temporary failure to sender.

discard
Accept object from sender, but drop it afterward.

reject Return permanent error to sender.

Please note, that the action 'discard' can be with ZMailer implemented only in a way, that the message is put into 'freezer'. It will end up in $POSTOFFICE/freezer, having the -3531 suffix.

LOGGING

Logging functionality of the ESETS agent modules has been developed to fine tune or to troubleshoot the agent module performance. Thus all the ESETS agent modules support only logging using syslogd daemon which logs system messages on *nix systems. To get more information on this topic please, refer to manual pages syslog(2), syslog.conf(5) and syslogd(8).

Regarding ESETS agent modules, this functionality can be invoked by setting ESETS module common configuration option *syslog_facility* to value other than **none**. To get description of the introduced ESETS module common configuration options please, refer to esets.cfg(5) manual page.

Once the syslog logging enabled, the ESETS agent module messages are logged with one of the following syslog priorities:

LOG_ERR
Error messages concerned with the ESETS agent module performance are logged with this priority. Message logged with this priority usually means that error occurred during the ESETS agent module running and thus the module could not accomplish its operation or even the module process exited.

LOG_WARNING
Warning messages concerned with the ESETS agent module performance are logged or 'summary' messages concerned with action other than 'accept' taken as a consequence of object scanning status are logged with this priority.

LOG_NOTICE
The 'summary' messages concerned with action taken as a consequence of object scanning status are logged with this priority.

LOG_INFO
The common tasks are logged with this priority.

LOG_DEBUG
Debug information concerned with the ESETS agent module performance is logged with this priority.

COMMAND LINE OPTIONS

This section contains list of command line options valid for this module.

Note that present version of ESETS implements in general three types of command line options parameters:

Integer parameters accept integer values, e.g.:

--integer-parameter 26

For integer parameter it is also possible to append unit K (1K = 1024), M (1M=1024*1024), G (1=1024*1024*1024), e.g.:

--integer-parameter 4K

Boolean (logical) parameters do not accept any arguments. Their appearance in the command line automatically signal enabling of an appropriate functionality related with the parameter, e.g.:

--bool-parameter

Thus in order to provide negation of an appropriate logical parameter prescribe this parameter with --no, e.g.:

--no-bool-parameter

String parameters accept string values. They can be put into quotation marks, e.g.:

--string-parameter "string value"

Besides options on the command line, there are also commands. All ESETS programs accept at least these commands for displaying the version number and a simple help screen.

-v, --version

Print version information to stdout and exit.

-h, --help

Print help screen to stdout and exit.

REPORTING BUGS

In order to report bugs, please visit http://www.eset.com/support <URL:http://www.eset.com/support> or use directly the support form at http://www.eset.eu/support/form <URL:http://www.eset.eu/support/form>.

COPYRIGHT

SEE ALSO

esets_cgp(1) esets_cli(1) esets_dac(1) esets_ftp(1) esets_gwia(1) esets_http(1) esets_icap(1) esets_imap(1) esets_mda(1) esets_mird(1) libesets_pac.so(1) esets_pipe(1) esets_pop3(1) esets_smfi(1) esets_smtp(1) esets_ssfi.so(1) esets_wwwi(1) esets_zmfi(1) esets(5) esets.cfg(5) esets_daemon(8) esets_inst(8)

esets_lic(8) esets_quar(8) esets_scan(8) esets_set(8) esets_update(8) eset_efs_userguide.pdf eset_egs_user-guide.pdf eset_ems_userguide.pdf