NAME

vfs_virusfilter - On access virus scanner

SYNOPSIS

vfs objects = virusfilter

DESCRIPTION

This is a set of various Samba VFS modules to scan and filter virus files on Samba file services with an anti-virus scanner.

This module is stackable.

OPTIONS

virusfilter:scanner

The antivirus scan-engine.

⊕

the Sophos AV scanner

⊕

the F-Secure AV scanner

⊕

the ClamAV scanner

virusfilter:socket path = PATH

Path of local socket for the virus scanner.

If this option is not set, the default path depends on the configured AV scanning engine.

For the *sophos* backend the default is */var/run/savdi/sssp.sock*.

For the *fsav* backend the default is */tmp/.fsav-0*.

For the *fsav* backend the default is */var/run/clamav/clamd.ctl*.

virusfilter:connect timeout = 30000

Controls how long to wait on connecting to the virus scanning process before timing out. Value is in milliseconds.

If this option is not set, the default is 30000.

virusfilter:io timeout = 60000
> Controls how long to wait on communications with the virus scanning process before timing out. Value is in milliseconds.

> If this option is not set, the default is 60000.

virusfilter:scan on open = yes
> This option controls whether files are scanned on open.

> If this option is not set, the default is yes.

virusfilter:scan on close = no
> This option controls whether files are scanned on close.

> If this option is not set, the default is no.

virusfilter:max file size = 100000000
> This is the largest sized file, in bytes, which will be scanned.

> If this option is not set, the default is 100MB.

virusfilter:min file size = 10
> This is the smallest sized file, in bytes, which will be scanned.

> If this option is not set, the default is 10.

virusfilter:infected file action = nothing
> What to do with an infected file. The options are nothing, quarantine, rename, delete.

> If this option is not set, the default is nothing.

virusfilter:infected file errno on open = EACCES
> What errno to return on open if the file is infected.

> If this option is not set, the default is EACCES.

virusfilter:infected file errno on close = 0
> What errno to return on close if the file is infected.

If this option is not set, the default is 0.

virusfilter:quarantine directory = PATH
 Where to move infected files. This path must be an absolute path.

 If this option is not set, the default is ".quarantine" relative to the share path.

virusfilter:quarantine prefix = virusfilter.
 Prefix for quarantined files.

 If this option is not set, the default is "virusfilter.".

virusfilter:quarantine suffix = .infected
 Suffix for quarantined files. This option is only used if keep name is true. Otherwise it is ignored.

 If this option is not set, the default is ".infected".

virusfilter:rename prefix = virusfilter.
 Prefix for infected files.

 If this option is not set, the default is "virusfilter.".

virusfilter:rename suffix = .infected
 Suffix for infected files.

 If this option is not set, the default is ".infected".

virusfilter:quarantine keep tree = yes
 If keep tree is set, the directory structure relative to the share is maintained in the quarantine directory.

 If this option is not set, the default is yes.

virusfilter:quarantine keep name = yes
 Should the file name be left unmodified other than adding a suffix and/or prefix and a random suffix name as defined in virusfilter:rename prefix and virusfilter:rename suffix.

 If this option is not set, the default is yes.

virusfilter:infected file command = @SAMBA_DATADIR@/bin/virusfilter-notify --mail-to

virusmaster@example.com --cc "%U@example.com" --from samba@example.com --subject-prefix
"Samba: Infected File: "
>   External command to run on an infected file is found.

>   If this option is not set, the default is none.

virusfilter:scan archive = true
>   This defines whether or not to scan archives.

>   Sophos and F-Secure support this and it defaults to false.

virusfilter:max nested scan archive = 1
>   This defines the maximum depth to search nested archives.

>   The Sophos and F-Secure support this and it defaults to 1.

virusfilter:scan mime = true
>   This defines whether or not to scan mime files.

>   Only the *fsav* scanner supports this option and defaults to false.

virusfilter:scan error command = @SAMBA_DATADIR@/bin/virusfilter-notify --mail-to
virusmaster@example.com --from samba@example.com --subject-prefix "Samba: Scan Error: "
>   External command to run on scan error.

>   If this option is not set, the default is none.

virusfilter:exclude files = empty
>   Files to exclude from scanning.

>   If this option is not set, the default is empty.

virusfilter:block access on error = false
>   Controls whether or not access should be blocked on a scanning error.

>   If this option is not set, the default is false.

virusfilter:scan error errno on open = EACCES
>   What errno to return on open if there is an error in scanning the file and block access on error is
>   true.

If this option is not set, the default is EACCES.

virusfilter:scan error errno on close = 0
>   What errno to return on close if there is an error in scanning the file and block access on error is
>   true.
>
>   If this option is not set, the default is 0.

virusfilter:cache entry limit = 100
>   The maximum number of entries in the scanning results cache. Due to how Samba's memcache
>   works, this is approximate.
>
>   If this option is not set, the default is 100.

virusfilter:cache time limit = 10
>   The maximum number of seconds that a scanning result will stay in the results cache. -1 disables
>   the limit. 0 disables caching.
>
>   If this option is not set, the default is 10.

virusfilter:quarantine directory mode = 0755
>   This is the octet mode for the quarantine directory and its sub-directories as they are created.
>
>   If this option is not set, the default is 0755 or S_IRUSR | S_IWUSR | S_IXUSR | S_IRGRP |
>   S_IXGRP | S_IROTH | S_IXOTH.
>
>   Permissions must be such that all users can read and search. I.E. don't mess with this unless you
>   really know what you are doing.

virusfilter:block suspected file = false
>   With this option on, suspected malware will be blocked as well. Only the *fsav*scanner supports
>   this option.
>
>   If this option is not set, the default is false.

NOTES

This module can scan other than default streams, if the alternative datastreams are each backed as
separate files, such as with the vfs module streams_depot.

For proper operation the streams support module must be before the virusfilter module in your vfs

objects list (i.e. streams_depot must be called before virusfilter module).

This module is intended for security in depth by providing virus scanning capability on the server. It is not intended to be used in lieu of proper client based security. Other modules for security may exist and may be desirable for security in depth on the server.

AUTHOR

The original Samba software and related utilities were created by Andrew Tridgell. Samba is now developed by the Samba Team as an Open Source project similar to the way the Linux kernel is developed.