NAME

semanage.conf – global configuration file for the SELinux Management library

DESCRIPTION

The **semanage.conf** file is usually located under the directory /etc/selinux and it is used for run-time configuration of the behavior of the SELinux Management library.

Each line should contain a configuration parameter followed by the equal sign ("=") and then followed by the configuration value for that parameter. Anything after the "#" symbol is ignored similarly to empty lines.

The following parameters are allowed:

module-store
Specify how the SELinux Management library should interact with the SELinux policy store. When set to "direct", the SELinux Management library writes to the SELinux policy module store directly (this is the default setting). Otherwise a socket path or a server name can be used for the argument. If the argument begins with "/" (as in "/foo/bar"), it represents the path to a named socket that should be used to connect the policy management server. If the argument does not begin with a "/" (as in "foo.com:4242"), it should be interpreted as the name of a remote policy management server to be used through a TCP connection (default port is 4242 unless a different one is specified after the server name using the colon to separate the two fields).

root Specify an alternative root path to use for the store. The default is "/"

store-root
Specify an alternative store_root path to use. The default is "/var/lib/selinux"

compiler-directory
Specify an alternative directory that contains HLL to CIL compilers. The default value is "/usr/lib/selinux/hll".

ignore-module-cache
Whether or not to ignore the cache of CIL modules compiled from HLL. It can be set to either "true" or "false" and is set to "false" by default. If the cache is ignored, then all CIL modules are recompiled from their HLL modules.

policy-version
When generating the policy, by default **semanage** will set the policy version to POLICYDB_VERSION_MAX, as defined in <sepol/policydb/policydb.h>. Change this setting if a different version needs to be set for the policy.

target-platform
The target platform to generate policies for. Valid values are "selinux" and "xen", and is set to "selinux" by default.

expand-check
Whether or not to check "neverallow" rules when executing all **semanage** command. It can be set to either "0" (disabled) or "1" (enabled) and by default it is enabled. There might be a large penalty in execution time if this option is enabled.

file-mode
By default the permission mode for the run-time policy files is set to 0644.

save-previous
It controls whether the previous module directory is saved after a successful commit to the policy store and it can be set to either "true" or "false". By default it is set to "false" (the previous version is deleted).

save-linked
It controls whether the previously linked module is saved (with name "base.linked") after a successful commit to the policy store. It can be set to either "true" or "false" and by default it is set to "false" (the previous module is deleted).

ignoredirs
List, separated by ";", of directories to ignore when setting up users homedirs. Some distributions use this to stop labeling /root as a homedir.

usepasswd
Whether or not to enable the use getpwent() to obtain a list of home directories to label. It can be set to either "true" or "false". By default it is set to "true".

disable-genhomedircon
It controls whether or not the genhomedircon function is executed when using the **semanage** command and it can be set to either "false" or "true". By default the genhomedircon functionality is enabled (equivalent to this option set to "false").

handle-unknown
This option controls the kernel behavior for handling permissions defined in the kernel but missing from the actual policy. It can be set to "deny", "reject" or "allow".

bzip-blocksize
It should be in the range 0-9. A value of 0 means no compression. By default the bzip block size is set to 9 (actual block size value is obtained after multiplication by 100000).

bzip-small
When set to "true", the bzip algorithm shall try to reduce its system memory usage. It can be set to either "true" or "false" and by default it is set to "false".

remove-hll
When set to "true", HLL files will be removed after compilation into CIL. In order to delete HLL files already compiled into CIL, modules will need to be recompiled with the **ignore-module-cache** option set to 'true' or using the **ignore-module-cache** option with semodule. The remove-hll option can be set to either "true" or "false" and by default it is set to "false".

Please note that since this option deletes all HLL files, an updated HLL compiler will not be able to recompile the original HLL file into CIL. In order to compile the original HLL file into CIL, the same HLL file will need to be reinstalled.

SEE ALSO

semanage(8)

AUTHOR

This manual page was written by Guido Trentalancia <guido@trentalancia.com>.

The SELinux management library was written by Tresys Technology LLC and Red Hat Inc.