NAME

selinux_set_callback − userspace SELinux callback facilities

SYNOPSIS

#include <selinux/selinux.h>

void selinux_set_callback(int *type***, union selinux_callback** *callback***);**

DESCRIPTION

selinux_set_callback() sets the callback indicated by *type* to the value of *callback*, which should be passed as a function pointer cast to type **union selinux_callback**.

All callback functions should return a negative value with *errno* set appropriately on error.

The available values for *type* are:

SELINUX_CB_LOG

int (**func_log***) (int** *type***, const char ****fmt***, ...);**

This callback is used for logging and should process the **printf**(3) style *fmt* string and arguments as appropriate. The *type* argument indicates the type of message and will be set to one of the following:

SELINUX_ERROR

SELINUX_WARNING

SELINUX_INFO

SELINUX_AVC

SELINUX_POLICYLOAD

SELINUX_SETENFORCE

SELINUX_ERROR, SELINUX_WARNING, and SELINUX_INFO indicate standard log severity levels and are not auditable messages.

The SELINUX_AVC, SELINUX_POLICYLOAD, and SELINUX_SETENFORCE message types can be audited with AUDIT_USER_AVC, AUDIT_USER_MAC_POLICY_LOAD, and AUDIT_USER_MAC_STATUS values from libaudit, respectively. If they are not audited, SELINUX_AVC should be considered equivalent to SELINUX_ERROR; similarly, SELINUX_POLICYLOAD and SELINUX_SETENFORCE should be considered equivalent to SELINUX_INFO.

SELINUX_CB_AUDIT

int (**func_audit***) (v oid ****auditdata***, security_class_t** *cls***,**
char ****msgbuf*, size_t** *msgbufsize***);**

This callback is used for supplemental auditing in AVC messages. The *auditdata* and *cls* arguments are the values passed to **avc_has_perm**(3). A human-readable interpretation should be printed to *msgbuf* using no more than *msgbufsize* characters.

SELINUX_CB_VALIDATE

int (**func_validate***) (char *****ctx***);**

This callback is used for context validation. The callback may optionally modify the input context by setting the target of the *ctx* pointer to a new context. In this case, the old value should be freed with **freecon**(3). The value of *errno* should be set to **EINVAL** to indicate an invalid context.

SELINUX_CB_SETENFORCE

int (**func_setenforce***) (int** *enforcing***);**

This callback is invoked when the system enforcing state changes. The *enforcing* argument indicates the new value and is set to *1* for enforcing mode, and *0* for permissive mode.

SELINUX_CB_POLICYLOAD

int (**func_policyload***) (int** *seqno***);**

This callback is invoked when the system security policy is reloaded. The *seqno* argument is the current sequential number of the policy generation in the system.

RETURN VALUE

None.

ERRORS

None.

AUTHOR

Eamon Walsh <ewalsh@tycho.nsa.gov>

SEE ALSO

selabel_open(3), **avc_init**(3), **avc_netlink_open**(3), **selinux**(8)