
sudo.conf

Fichier de configuration de sudo

sudo.conf supporte les directive 'Plugin', 'Path', 'Set', 'Debug'.

Plugin

Une ligne Plugin définit un module et son chemin, suivi de paramètres optionnels. Peut être spécifié plusieurs fois

Plugin sudoers_policy /usr/local/libexec/sudo/sudoers.so sudoers_mode=0440

Path

Path définit les chemins vers divers bibliothèques/programmes nécessaires. Si une ligne Path ne contient pas de chemin, la fonctionnalité est considérée désactivée :

askpass chemin du helper pour lire les mots de passe quand aucun terminal n'est disponible

noexec Chemin de la bibliothèque wrappers pour les fonctions execl(), execl(), execlp(), exect(), execv(), execve(), execvp(), execvp(), execvpe(), fexecve(), popen(), posix_spawn(), posix_spawn(), system(), et wordexp() qui empêche l'exécution d'autres commandes. Utilisé pour implémenter la fonctionnalité noexec dans les systèmes qui supportent LD_PRELOAD ou son équivalent.

plugin_dir Répertoire de recherche des plugins spécifier sans chemin complet.

sesh Chemin de sesh. Utilisé quand sudo est compilé avec le support SELinux

Set

disable_coredump true|false Par défaut sudo désactive le coredump pour éviter toute fuite de données sensible

group_source sudo passe la liste des groupes de l'utilisateur invoquant à la stratégie et les plugins I/O. Dans la plupart des systèmes, il y a une limite du nombre de groupes (généralement 16). Si la liste de groupe dépasse la limite kernel, sudo consulte lui-même la liste des groupes :

static Utilise la liste de groupe statique que le kernel retourne

dynamic Requête toujours la base de groupe. C'est dynamique dans le sens où les changements faits dans la base de groupe après que l'utilisateur se soit loggé sont reflétés dans la liste des groupes.

adaptive Ne requête la base que si la liste des groupes retournés par le kernel a atteint la limite des entrées.

max_groups Nombre maximum de groupes utilisateur à récupérer dans la base de groupe lorsque sudo requête la base de groupe directement

probe_interfaces Par défaut, sudo sonde les interfaces réseaux du système et passe l'IP à chaque interface activée au plugin de stratégie. Cela simplifie les règles de match basées sur l'IP sans avoir à requêter DNS.

Debug

Une ligne Debug consiste du mot clé Debug, suivi par le nom du programme ou plugin à déboguer (sudo, visudo, sudoreplay, sudoers), le nom du fichier de débog et une liste de flags. Par exemple :

Debug sudo /var/log/sudo_debug all@warn,plugin@info

all Match tous les sous-systèmes
args traitement des arguments de la ligne de commande
conv Conversation utilisateur
edit sudoedit
event Sous-système d'évènement
exec exécution de commande
main Fonction main de sudo
netif Gestion des interfaces réseaux
pcomm Communication avec le plugin
pty Code lié au pty
selinux gestion SELinux
util Fonctions utilitaires
utmp Gestion utmp