pam_namespace

Définit un espace de nom privé

pam_namespace définit un espace de nom privé pour une session avec répertoire poly-instancés. Un répertoire poly-instancié fournis une instance différente de lui-même basé sur le nom utilisateur, ou en utilisant SELinux, le nom d'utilisateur, contexte de sécurité ou les 2. Si un script exécutable **/etc/security/namespace.init** existe, il est utilisé pour initialiser l'instance du répertoire après qu'il ai été définis et monté dans le répertoire poly-instancié. Le script reçoit le chemin du répertoire poly-instancié, le chemin du répertoire instance, si le répertoire instance a été nouvellement crée (0 pour non, 1 pour oui), et le nom de l'utilisateur.

Le module dissocie l'espace de nom de session du parent. Un **mount/umount** est effectué dans l'espace de nom du parent.

/etc/security/namespace.conf spécifie quels répertoires sont poly-instanciés, comment ils sont poly-instanciés, comment l'instance sera nommé, et les utilisateurs pour qui la poly-instatiation sera effectuée.

Le format de **/etc/security/namespace.conf** :

polydir instance_prefix method list_of_uids

polydir est un chemin absolu du répertoire à poly-instancier. La chaîne $HOME est remplacée avec le home de l'utilisateur, et $USER par le nom d'utilisateur. Ce champs ne peut pas être vide

instance_prefix chaîne utilisée pour construire le chemin pour l'instanciation de polydir. En fonction de la méthode de poly-instanciation

method est la méthode utilisée pour la poly-instanciation. Ce champs ne peut pas être vide. Peut être :

user pour une poly-instaciation basé sur le nom d'utilisateur

level pour une poly-instanciation basé sur le niveau MLS sur processus et le nom d'utilisateur

context pour une poly-instanciation basé sur le contexte de sécurité du processus et le nom d'utilisateur

tmpfs pour monter le système de fichier tmpfs comme instance de répertoire

tmpdir pour créer un répertoire temporaire comme instance de répertoire qui est supprimé quand l'utilisateur ferme sa session

context et level sont disponible uniquement avec SELinux.

list_of_uids est une liste séparée par une virgule de noms d'utilisateurs pour qui la poly-instanciation n'est pas effectuée. Si ce champs est vide, s'effectue pour tous les utilisateurs si la liste est précédée par " ", la poly-instanciation est effectuée uniquement pour les utilisateurs dans la liste.

method peut aussi contenir les flags optionnels suivant :

create=mode,owner,group crée le répertoire poly-instancié. Les paramètres sont optionnels. Par défaut le **mode** est déterminé par umask, **owner** est l'utilisateur et **group** est le groupe de l'utilisateur.

iscript=path chemin du script d'init.

noinit Le script d'init ne sera pas exécuté

shared les répertoire instanciés pour les méthodes "context" et "level" ne contiendrons pas le nom d'utilisateur et seront partagés à tous les utilisateurs.

Le répertoire où les instances poly-instanciées sont créées, doit exister et doit avoir, par défaut, le mode 0000. Cela nécessite que le parent de l'instance soit de mode 0000 et puisse être écrasé avec l'option de ligne de commande **ignore_instance_parent_mode**

Avec les méthodes **context** et **level**, le contexte SELinux qui est utilisé est le contexte utilisé pour exécuter un nouveau processus comme obtenus par **getexeccon**. Ce contexte doit être définis par l'application appelante ou le module pam_selinux.so. Si ce contexte n'est pas définis la poly-instaciation sera basé uniquement sur le nom d'utilisateur.

OPTIONS

debug syslog les informations de debuggage

unmnt_remnt Pour les programmes comme su et newrole, le login session a déjà définis un espace de nom poly-instancié. Pour ces programmes, la poly-instanciation est effectuée basé sur le nouveau user id ou le contexte de sécurité, cependant la commande a d'abord besoin d'annuler la poly-instanciation effectuée par login. Cet argument instruit la commande d'annuler d'abord la précédente poly-instanciation avant de traiter avec la nouvelle basé sur le nouveau id/context

unmnt_only Pour les programmes de confiance qui veulent annuler un mount existant et traiter les répertoires instanciés, cet argument leur permet de démonter une instance actuellement montée.

require_selinux si SELinux n'est pas activé, retourne une erreur

gen_hash Au lieu d'utiliser la chaîne de contexte de sécurité pour le nom de l'instance, génère et utilise son hash md5

ignore_config_error Si une ligne dans le fichier de configuration correspondant à un répertoire poly-instancié contient une erreur de format, ignore le traitement de la ligne suivante. Sans cette option, pam va retourner une erreur au programme appelant, forçant à terminer la session

ignore_instance_parent_mode Les répertoires parents sont supposés avec le mode 000. En utilisant cette option, un administrateur peut choisir d'ignorer le mode du parent. À utiliser avec précaution vu que cela réduit le but d'isolation et de sécurité de la poly-instanciation

no_unmount_on_close Pour certain programmes de confiance comme newrole, la session ouverte est appelée depuis un processus enfant alors que le parent ferme la session. Pour ces commandes, utiliser cette option pour instruire pam_close_session de ne pas démonter le répertoire poly-instancié dans la parent.

use_current_context utile pour les services qui n'utilisent pas pam_selinux pour changer le contexte SELinux avec l'appel setexeccon. Le module va utiliser le contexte SELinux par défaut de l'utilisateur pour la poly-instanciation level et context

ne fournis que le type de module session. Ce module ne doit pas être appelé depuis un processus multithread.

Valeurs retournées

PAM_SUCCESS espace de nom définit avec succès

PAM_SERVICE_ERR erreur inattendue

PAM_SESSION_ERR erreur de configuration inattendue

Exemples

exemple de ligne dans /etc/security/namespace.conf
/tmp /tmp-inst/ level root,adm
/var/tmp /var/tmp/tmp-inst/ level root,adm
$HOME $HOME/$USER.inst/inst- context
ligne à placer dans une fichier de config
session required pam_namespace.so [arguments]