
pam_radius_auth

Authentification auprès d'un serveur Radius

OPTIONS

debug syslog des informations détaillées

use_first_pass Récupère le mot de passe depuis un précédent module. S'il ne peut récupérer de mot de passe, échoue.

try_first_pass Récupère le mot de passe depuis un précédent module. S'il ne peut récupérer de mot de passe, le demande à l'utilisateur

skip_passwd Ne demande pas de mot de passe, même si aucun n'a été trouvé. envoie le précédent s'il en existe un ou envoie un mot de passe NULL.

conf=foo Fichier de configuration à utiliser. défaut : /etc/raddb/server

client_id=bar Envoie un Attribut RADIUS NAS-Identifiant avec la chaîne spécifiée. si client_id n'est pas spécifié, le type PAM_SERVICE est utilisé ('login', 'su', 'passwd', etc.) Peut être désactivé avec client_id=

retry=# Définit le nombre de tentatives.

use_authok Force l'utilisation d'un mot de passe précédemment entré. Nécessaire pour la vérification de la complexité des mots de passe, par exemple, en utilisant cracklib.

ruser si PAM_USER est root, utilise la valeur de PAM_RUSER au lieu de PAM_USER pour déterminer le nom d'utilisateur à authentifier via RADIUS. Cela permet à su d'agir comme sudo

localifdown retourne PAM_IGNORE au lieu de PAM_AUTHINFO_UNAVAIL si RADIUS auth échoue à cause d'une indisponibilité réseau.

accounting_bug Utilisé, le vecteur de réponse de compte n'est pas validé. (pour la compatibilité de très vieux serveur RADIUS)

Exemples

auth sufficient /lib/security/pam_radius_auth.so

account sufficient /lib/security.pam_radius_auth.so