

Firepower 4100/9300 FXOS Récupération de mot de passe utilisateur local via TACACS Accès administratif

Table des matières

Problème

Le mot de passe d'administration local pour FXOS sur les appliances Firepower 4100/9300 était inconnu et devait être réinitialisé pour pouvoir récupérer l'accès administratif.

Tous les utilisateurs TACACS existants se sont uniquement vu attribuer le rôle Lecture seule, ce qui les a empêchés d'effectuer des tâches administratives sur le châssis FXOS.

Remarque : les comptes d'utilisateurs authentifiés à distance (LDAP, RADIUS, TACACS+, SSO) se voient attribuer le rôle Lecture seule par défaut.

Environnement

- Cisco Firepower 4100/9300 exécutant ASA/FTD
- Authentification FXOS par défaut définie sur distant (Cisco ISE) ; authentification locale configurée comme mode de secours.

Résolution

Créer un utilisateur TACACS administratif

Sur Cisco ISE (ou votre serveur TACACS), créez un nouvel utilisateur TACACS (par exemple, fxosadmin) et attribuez des privilèges d'administration comme indiqué dans la documentation Cisco :

[Authentification/autorisation du châssis FXOS pour la gestion à distance avec ISE à l'aide de TACACS+.](#)

1. Créer les groupes d'identités et les utilisateurs
2. Créez le profil Shell pour chaque rôle utilisateur (pour le rôle 'admin', utilisez cisco-av-pair=shell : roles="admin")
3. Créer la stratégie d'autorisation TACACS

Connectez-vous à l'aide du nouvel utilisateur Admin TACACS

Utilisez le nouveau compte fxosadmin pour vous connecter à l'interface graphique utilisateur et à l'interface de ligne de commande de FXOS. Ce compte dispose maintenant de privilèges d'administration complets.

Réinitialiser le mot de passe administrateur local

Accédez à l'interface de ligne de commande FXOS et exécutez ces commandes :

```
FP4100# scope security
FP4100 /security # show local-user
User Name      First Name      Last name
-----
admin
FP4100 /security # enter local-user admin
FP4100 /security/local-user # set password
Enter a password:
Confirm the password:
FP4100 /security/local-user* # commit-buffer
FP4100 /security/local-user #
```

Remarques et considérations

- Lorsque l'authentification à distance (TACACS, RADIUS, LDAP, SSO) est la méthode par défaut, vous ne pouvez pas vous connecter au Gestionnaire de châssis de pare-feu avec un compte d'utilisateur local, sauf si l'authentification à distance n'est pas disponible.
- Les comptes d'utilisateurs locaux et distants ne peuvent pas être utilisés de manière interchangeable lorsque l'authentification distante est active.
- Dans le scénario, si la méthode d'authentification du port de console est définie sur « LOCAL », elle permet de vérifier les nouvelles informations d'identification de l'administrateur, sinon vous devez désactiver la connectivité du serveur d'authentification distant pour tester les informations d'identification de l'administrateur.

Motif

- Le mot de passe d'administrateur local du châssis FXOS a été perdu ou inconnu, ce qui empêche l'accès administratif direct à l'aide du compte local.
- Tous les comptes d'utilisateurs TACACS existants ont été configurés avec des privilèges de lecture seule, ce qui a limité la possibilité d'effectuer les tâches administratives nécessaires, telles que le redémarrage du châssis, les mises à niveau, la sauvegarde FXOS, à partir de l'accès à distance.
- Cette situation risquait de ne pas permettre la gestion ou la récupération du périphérique si d'autres modifications ou dépannages étaient nécessaires.
- Cela a nécessité une réinitialisation du mot de passe admin pour poursuivre les activités de maintenance planifiées.

Autres informations utiles

- [Gestion des utilisateurs FXOS](#)
- [Procédure De Récupération De Mot De Passe Pour Les Appareils Firepower 9300/4100](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.