Dépannage de l'échec d'authentification SSH sur ASA avec RADIUS en utilisant un mot de passe unique

Table des matières

Problème

L'accès SSH (Secure Shell) au logiciel ASA (Adaptive Security Appliance) avec RADIUS (Remote Authentication Dial-In User Service) à l'aide d'un mot de passe à usage unique (OTP) échoue lorsque la pile CiscoSSH est activée.

Les messages syslog suivants sont générés :

```
Nov 14 2025 16:28:35: %ASA-6-113010: AAA challenge received for user from server .
Nov 14 2025 16:28:35: %ASA-4-109033: Authentication failed for admin user from . Interactive challenge
```

Environnement

Les symptômes sont observés lorsque toutes les conditions correspondent :

- Pare-feu sécurisé 1230 avec ASA en mode mono ou multicontexte. D'autres plates-formes matérielles sont également concernées.
- Le serveur RADIUS est utilisé pour l'authentification SSH :

<#root>

```
device#
```

show run | i aaa

```
aaa-server RAD-OTP protocol radius
aaa-server RAD-OTP (management) host 192.0.2.1
aaa-server RAD-OTP (management) host 192.0.2.2
aaa authentication ssh console RAD-OTP
```

- Le serveur RADIUS demande et requiert un code OTP ou une demande de confirmation valide pour une authentification réussie.
- La pile CiscoSSH est activée sur ASA.
- Dans les versions 9.19.1 et ultérieures, la pile CiscoSSH est activée par défaut et peut être désactivée en option à l'aide de la commande no ssh stack cisco. Utilisez la commande show ssh pour la vérification :

<#root>

```
device#

show ssh


ssh secure copy : ENABLED

ciscoSSH stack : DISABLED
```

- Dans les versions 9.23.1 et ultérieures, cette pile ne peut pas être désactivée ou vérifiée.

Résolution

Les symptômes sont reproduits avec succès dans le laboratoire interne et suivis dans l'ID de bogue Cisco CSCwt5790.

Utilisez l'une de ces options de contournement dans les versions concernées :

- Utiliser l'authentification locale pour les connexions SSH.
- Sur le serveur RADIUS, désactivez la configuration OTP requise pour ASA.
- Dans les versions antérieures à la version 9.23, désactivez la pile CiscoSSH à l'aide de la commande no ssh stack cisco. Assurez-vous d'examiner la référence des commandes de la

gamme Cisco Secure Firewall ASA, les commandes S et d'évaluer l'impact potentiel de la désactivation de la pile CiscoSSH.

Motif

La cause de l'échec d'authentification est l'ID de bogue Cisco CSCwt5790.

Autres informations utiles

- ID de bogue Cisco CSCwi04513
- ID de bogue Cisco CSCwt57790
- Référence des commandes de la gamme Cisco Secure Firewall ASA, commandes S

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.