

Résoudre le délai de connexion LDAP de migration cloud AWS de la passerelle de messagerie sécurisée

Table des matières

Problème

Après avoir migré l'environnement Cisco Secure Email Gateway (SEG) vers la plate-forme Amazon Web Services (AWS) hébergée dans le cloud, les administrateurs rencontrent des problèmes persistants de connexion et de performances.

Symptômes inclus :

- Délais importants lors de l'accès au SEG dans les interfaces GUI et CLI
- Temps excessif requis pour l'authentification après la saisie du nom d'utilisateur et du mot de passe
- Chargement très lent du tableau de bord principal/page
- La réactivité globale de la plate-forme était extrêmement lente
- Les problèmes étaient les plus évidents lors de l'accès authentifié LDAP

L'analyse de capture de paquets révèle que les sessions TCP SEG vers les serveurs LDAP sont fermées par l'équilibreur de charge de passerelle (GWLb) après environ 350 secondes d'inactivité, ce qui entraîne des délais d'authentification et des délais d'expiration.

Environnement

- Migration de Cisco Secure Email Gateway (SEG) vers une plate-forme hébergée dans le cloud AWS

- Version AsyncOS : 16.0.4-016
- Authentification LDAP configurée avec Active Directory
- Équilibreur de charge de passerelle AWS (GWLB) dans le chemin d'accès réseau
- Cisco Secure Email and Web Manager est également affecté par le même problème
- Cryptage SSL/TLS activé pour les connexions LDAP sur le port 3269

Résolution

Ajustez les paramètres de durée de vie de connexion LDAP pour empêcher les délais d'inactivité de session provoqués par l'équilibreur de charge de la passerelle AWS en procédant comme suit :

1. Connectez-vous à l'interface de ligne de commande SEG et accédez à la configuration LDAP :

```
device# ldapconfig
```

2. Localisez le profil de serveur LDAP et modifiez le paramètre « Durée de vie maximale par connexion au serveur (en secondes) ». Modifiez cette valeur en 300 secondes pour vous assurer que les connexions sont actualisées avant le seuil de délai d'inactivité de 350 secondes de l'équilibreur de charge de passerelle.

Configuration initiale :

```
Max lifetime per connection: 1800
```

Configuration mise à jour :

```
Max lifetime per connection: 300
```

3. Validez les modifications de configuration et autorisez le système à appliquer les nouveaux paramètres.

4. Appliquez la modification de durée de vie de connexion LDAP identique à Cisco Secure Email and Web Manager en utilisant la même configuration de 300 secondes.
5. Testez la fonctionnalité de connexion de l'interface graphique et de la CLI. Une fois les modifications implémentées, les temps de connexion doivent être réduits à environ 5 secondes et les délais d'authentification ne doivent plus se produire.
6. Surveillez l'environnement pour détecter toute récurrence du problème et collectez des captures de paquets si les problèmes persistent.

Motif

L'analyse de capture de paquets a montré que l'équilibreur de charge de passerelle AWS (GWLB) mettait fin aux sessions TCP inactives après environ 350 secondes. La durée de vie de la connexion LDAP par défaut du SEG est de 1800 secondes, ce qui dépasse le seuil de délai d'inactivité de GWLB de 350 secondes. Lorsque les connexions LDAP restaient inactives pendant plus de 350 secondes, le GWLB interrompait les sessions TCP, ce qui provoquait des délais d'authentification et des délais d'expiration lorsque les utilisateurs tentaient de se connecter. En réduisant la durée de vie de la connexion LDAP à 300 secondes, le SEG actualise les connexions de manière proactive avant que le délai d'attente GWLB ne se produise et empêche les retards d'authentification.

Autres informations utiles

- [Guide de l'utilisateur d'AsyncOS 16.5 pour Cisco Secure Email Cloud Gateway - GD \(General Deployment\)](#)
- [Guide de l'utilisateur d'AsyncOS 16.5 pour Cisco Secure Email and Web Manager - GD \(General Deployment\)](#)

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.