

Erreur ISE SFTP RSA Key Authentication Timeout

Table des matières

Problème

Un référentiel SFTP configuré avec l'authentification par clé RSA fonctionne correctement sur un noeud ISE (ise1) mais échoue sur un autre noeud ISE (ise2) exécutant ISE 3.4. Sur le noeud défaillant, la connexion SSH et la validation du serveur se terminent correctement, mais l'authentification par clé publique ne se termine pas et la session SFTP expire avec une erreur « sftp_select : délai d'attente !" .

Lorsque vous essayez de lister le contenu du référentiel SFTP à l'aide de la commande show repository SFTP sur le noeud ISE affecté, cette séquence d'erreurs se produit :

```
device/admin# show repository SFTP
6 [4005534]:[info] transfer: cars_xfer.c[333] [system]: sftp dir of repository SFTP requested
6 [4005534]:[info] transfer: cars_xfer_util.c[2654] [system]: Server validation successful 10.50.60.200
7 [4005534]:[debug] transfer: sftp_handler.c[1295] [system]: Running sftp command: 10.50.60.200 will.ki
6 [4005534]:[info] transfer: sftp_handler.c[695] [system]: DEBUG: local user: admin UID: 0 sftp_run_par
7 [4005534]:[debug] transfer: sftp_handler.c[705] [system]: fd is:7
7 [4005535]:[debug] transfer: sftp_handler.c[327] [system]: Executing SFTP command: 0 admin /usr/bin/sf
3 [4005534]:[error] transfer: sftp_handler.c[417] [system]: sftp_select Error: timeout!
7 [4005534]:[debug] transfer: sftp_handler.c[1136] [system]: sftp parent status -999
% Failure occurred during request
```

Cela empêche l'utilisation du référentiel SFTP à partir du noeud ISE affecté pour des fonctions ISE critiques telles que les opérations de sauvegarde.

Environnement

- Cisco Identity Services Engine (ISE) version 3.4.0
- Déploiement ISE multinoeud avec au moins deux noeuds (ise1 et ise2)

- Référentiel SFTP configuré avec authentification par clé RSA
- Authentification SSH basée sur des clés utilisant une clé privée RSA (/home/admin/.ssh/id_rsa)
- Serveur SFTP accessible
- Authentification par mot de passe désactivée (-oPasswordAuthentication=no)

Résolution

Cette affaire fait actuellement l'objet d'une enquête par l'équipe technique. Le problème a été transmis pour l'analyse du journal racine afin de déterminer la cause sous-jacente du délai d'attente SFTP sur le noeud ISE affecté.

En fonction des résultats du débogage, effectuez les étapes de dépannage décrites dans les sections suivantes pour collecter des informations supplémentaires.

Étape 1: Vérifier la cohérence de la configuration du référentiel SFTP entre les noeuds

Comparez la configuration du référentiel SFTP sur les deux noeuds ISE pour vous assurer qu'ils sont identiques.

Étape 2: Vérifier les autorisations et la propriété des fichiers de clé SSH

Vérifiez que le fichier de clé privée SSH (/home/admin/.ssh/id_rsa) dispose des autorisations et de la propriété correctes sur le noeud affecté.

Étape 3: Tester la connectivité réseau

Vérifiez que le noeud ISE affecté peut atteindre le serveur SFTP sur le port 22 et qu'il n'y a aucun problème de blocage au niveau du réseau.

Étape 4: Activer le débogage supplémentaire

Activez un débogage SSH/SFTP plus détaillé pour capturer des informations détaillées sur l'échec de l'authentification.

À partir de la CLI du noeud affecté :

1.- Activez ces débogages avec des commandes :

- debug copy 7
- debug transfer 7

2.- Utilisez la commande show repository xxxxx après avoir activé les débogages pour capturer plus d'informations.

Étape 5: Comparer les empreintes des clés SSH

Vérifiez que la clé publique SSH sur le serveur SFTP correspond à la clé privée utilisée par le noeud ISE affecté.

Le problème a été résolu en identifiant la phrase de passe correcte utilisée pour générer la clé RSA sur le noeud SPAN et en reconfigurant les paramètres du référentiel pour les aligner avec les informations d'identification valides.

Solution de contournement provisoire

Il est conseillé de vérifier manuellement la phrase de passe à l'aide de ssh-keygen -y -f /home/admin/.ssh/id_rsa sur l'interface de ligne de commande pour confirmer le mot de passe qui a déverrouillé la clé privée avant de réappliquer la configuration du référentiel dans l'interface graphique utilisateur.

Étapes de régénération de la clé RSA :

1.- Ouvrez l'interface de ligne de commande du noeud concerné.

2.- Supprimez l'ancienne clé RSA avec la commande `crypto key delete rsa`.

3.- Générez une nouvelle clé RSA avec la phrase de passe souhaitée avec la commande `crypto key generate rsa passphrase XXXXXXXXXXXXXXXX`.



Remarque : La phrase de passe doit comporter au moins 13 caractères.

4.- Obtenez la nouvelle clé publique RSA à importer dans l'autre système avec la commande `show crypto key`.

Motif

Erreur utilisateur / Erreur de configuration. L'enquête a déterminé que l'échec de l'authentification du référentiel sur le noeud secondaire était causé par une non-correspondance entre la phrase de passe attendue et la phrase de passe utilisée pour sécuriser la clé privée RSA stockée. Cela a empêché le sous-système de chiffrement de déchiffrer correctement la clé pour signer la demande d'authentification SSH.

Autres informations utiles

- [Assistance technique de Cisco et téléchargements](#)

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.