Dépannage de l'authentification de clé publique SSH StarOS

Table des matières

Introduction

Ce document décrit comment dépanner la configuration d'authentification de clé publique SSH/SFTP de la passerelle de paquets vers les serveurs externes dans StarOS.

Problème

Si des messages d'avertissement ou d'échec apparaissent après la génération et la configuration de clés publiques, consultez la section suivante pour connaître les solutions possibles.

Solution

- Des clés client SSH sont-elles présentes ?

Recherchez la clé publique SSH à l'aide de l'interface de ligne de commande « show ssh client key ». Si les clés ne sont pas présentes, générez-les à l'aide de l'ensemble des CLI présentes dans la section « Génération des clés SSH » du document de référence dans la section de référence ci-dessous.

Ensuite, authentifiez les clés à transmettre au serveur distant à l'aide de l'interface de ligne de commande d'exécution « push ssh-key <hostname> user <username> [context <contextname>].

- Avez-vous appuyé sur la clé SSH du client ?

Si la clé publique SSH du client n'est pas présente dans la liste autorisée du serveur distant, poussez la clé publique vers le serveur distant à l'aide de l'interface de ligne de commande d'exécution « poussez la clé ssh <nom d'hôte> utilisateur <nom d'utilisateur> [contexte <nom du contexte>].

- Le serveur distant prend-il en charge l'authentification par clé publique ?

Vérifiez que le serveur distant prend en charge l'authentification par clé publique en consultant le fichier de configuration SSHD du serveur distant. Assurez-vous que le paramètre « PubkeyAuthentication yes » est présent dans le fichier de configuration SSHD.

Si des modifications sont apportées aux paramètres/valeurs dans le fichier de configuration SSHD, le serveur SSHD doit être redémarré pour être effectif.

- Voyez-vous des messages d'avertissement ou d'échec ?

« Avertissement : fichier d'ID introuvable » :

Cela indique que les fichiers d'ID des clés du client SSH sont manquants en raison d'une erreur interne ou de la suppression manuelle des fichiers. Les actions à restaurer sont les suivantes.

- Si l'o/p de l'interface de ligne de commande d'exécution « show ssh client key [type v2-rsa] » affiche la clé publique v2-rsa au format « hex » et « bubble-babble » et affiche en outre le message d'échec « Failure : Unable to find ssh public key file », alors,
    1. Obtenez/sauvegardez la clé du client SSH (ssh key **<key>** len **<keylen>** type v2-rsa) à partir de la section de configuration du client SSH (« client ssh ») de l'interface de ligne de commande d'Exec « show configuration » o/p.
    2. Reconfigurez la même valeur de clé SSH en passant en mode CLI « config-ssh ».
    3. Exemple :

<#root>

```
[local]swch#
```

show ssh client key type v2-rsa

```
v2-rsa public key:
    ximal-hyges-hovul-vonuk-lacyl-pezuk-nifad-lulon-raviv-cypal-vyxox
    60:75:d1:c5:7a:7e:e7:67:86:7a:7d:69:0e:27:5d:9b:78:e1:69:7e
"Failure: Unable to find ssh public key file"

[local]swch#
```

show configuration

config

….

client ssh

ssh key +KEYVALUE len KEYLEN type v2-rsa

```
#exit
```

…

```
[local]swch61#
configure

[local]swch61(config)#
client ssh

[local]swch61(config-ssh)#
ssh key +KEYVALUE len KEYLEN type v2-rsa

[local]swch61(config-ssh)#
end
```

Si ces avertissements s'affichent, contactez le support technique Cisco.

```
“Warning: Failed to add ID file argument”
“Warning: Failed to add ciphers argument”
“Warning: Failed to add preferred authentication argument”
“Failure: Failed to add ssh options”
```

Référence:

Guide d'administration du système VPC-DI, StarOS version 21.28

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.