Dépannage de l'échec de la connexion de SEG au cluster en raison d'une erreur de clé correspondante

Table des matières

Introduction

Ce document décrit comment dépanner une passerelle de messagerie sécurisée (SEG) qui ne peut pas rejoindre un cluster existant.

Prérequis

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment joindre des appliances dans un cluster (gestion centralisée).
- Tous les ESA doivent avoir les mêmes versions AsyncOS (jusqu'à la révision).

Exigences

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous que vous comprenez le potentiel de toute commande

Problème

Le problème se produit lors de l'ajout d'une passerelle de messagerie sécurisée (SEG) à un cluster existant. Le problème provoque une erreur sur la connexion, ceci est dû à l'ESA manque certains des algorithmes kex / algorithmes de chiffrement.

Impossible de joindre le cluster.
Erreur : "(3, 'Impossible de trouver l'algorithme d'échange de clés correspondant.')"
Saisissez l'adresse IP d'une machine dans le cluster.

Solution

Il est nécessaire d'utiliser les valeurs par défaut pour sshconfig

<#root>

```
esa> sshconfig


Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
- ACCESS CONTROL - Edit SSH whitelist/blacklist
[]> sshd


ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
```

Pour appliquer les valeurs par défaut, vous pouvez exécuter la commande à partir de la CLI **>** sshconfig **>** sshd sur la configuration pas à pas :

<#root>

```
[]> setup

Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]>
```

rsa1,ssh-dss,ssh-rsa

```
Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc]>
```

aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijn

aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijn

```
Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160]>
```

hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-9

```
Enter the Minimum Server Key Size do you want to use
[1024]>

Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1]>
```

diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1

,

diffie-hellman-group14-sha1

,

iffie-hellman-group1-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

Valider les modifications

```
esa> commit

Please enter some comments describing your changes:

[]> Edit the SSHD values
```

Une fois la modification effectuée, l'appliance se connecte au cluster avec succès

Informations connexes

Configurer un cluster ESA (Email Security Appliance)

FAQ ESA : Quelles sont les conditions requises pour la configuration d'un cluster ?

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.