Probleemoplossing: SEG niet toetreden tot cluster vanwege bijbehorende sleutelfout

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij een beveiligde e-mailgateway (SEG) die niet kan worden toegevoegd aan een bestaand cluster.

Vereist

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe u apparaten kunt samenvoegen tot een cluster (gecentraliseerd beheer).
- Alle ESA's moeten dezelfde AsyncOS-versies hebben (tot aan de herziening).

Vereisten

De informatie in dit document is gemaakt op basis van de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, zorg er dan voor dat u het potentieel van elke opdracht begrijpt

Probleem

Het probleem bestaat wanneer u zich aanmeldt bij een Secure Email Gateway (SEG) voor een bestaand cluster. Het probleem veroorzaakt een fout bij de verbinding, dit komt doordat de ESA enkele kex algoritmen / algoritmen mist.

Kan zich niet bij het cluster aansluiten.
Fout was: "(3, 'Kan geen overeenkomend sleuteluitwisselingsalgoritme vinden.')"
Voer het IP-adres van een machine in het cluster in.

Oplossing

De standaardwaarden voor shconfig moeten worden gebruikt

<#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
```

Om de standaardwaarden toe te passen kunt u de opdracht uitvoeren vanaf de CLI **>** shconfig **>** sshd op de stapsgewijze instelling:

<#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

De wijzigingen doorvoeren

esa> commit

Please enter some comments describing your changes:

[]> Edit the SSHD values

Na de wijziging sluit het apparaat zich met succes aan bij het cluster

Gerelateerde informatie

[Cluster voor e-mail security applicatie (ESA) configureren]

[ESA FAQ: Wat zijn de vereisten voor het opzetten van een cluster?]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.