Solución de problemas de error al unir SEG al clúster debido a un error de clave coincidente

Contenido

Introducción

Este documento describe cómo resolver problemas de un Secure Email Gateway (SEG) que no puede unirse a un clúster existente.

Requisito previo

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo unir dispositivos en un clúster (administración centralizada).
- Todos los ESA deben tener las mismas versiones de AsyncOS (hasta la revisión).

Requirements

La información de este documento se creó a partir de los dispositivos en un entorno de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está activa, asegúrese de comprender el potencial de cualquier comando

Problema

El problema existe al unir un gateway de correo electrónico seguro (SEG) a un clúster existente. El problema indica un error en la conexión, esto se debe a que el ESA no tiene algunos de los algoritmos kex/algoritmos cipher.

No se pudo unir al clúster.
Error: "(3, 'No se pudo encontrar el algoritmo de intercambio de claves coincidente.')"
Introduzca la dirección IP de una máquina en el clúster.

Solución

Es necesario utilizar los valores predeterminados para 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
```

Para aplicar los valores predeterminados, puede ejecutar el comando desde CLI > sshconfig > sshd en la configuración paso a paso:

<#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

Registrar los cambios

```
esa> commit

Please enter some comments describing your changes:

[]> Edit the SSHD values
```

Después del cambio, el dispositivo se une al clúster correctamente

Información Relacionada

[Configuración de un clúster de dispositivos de seguridad de correo electrónico (ESA)]

[Preguntas frecuentes sobre ESA: ¿Cuáles son los requisitos para configurar un clúster?]

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).