Troubleshooting de Falha ao Ingressar o SEG no Cluster Devido a Erro de Chave Correspondente

Contents

Introdução

Este documento descreve como solucionar problemas de um Secure Email Gateway (SEG) que não pode ingressar em um cluster existente.

Pré-requisito

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como unir dispositivos em um cluster (gerenciamento centralizado).
- Todos os ESAs devem ter as mesmas versões do AsyncOS (até a revisão).

Requisitos

As informações neste documento foram criadas a partir dos dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que você compreende o potencial de qualquer comando

Problema

O problema ocorre ao ingressar em um Secure Email Gateway (SEG) em um cluster existente. O problema provoca um erro na conexão, isso se deve à ausência do ESA de alguns algoritmos/algoritmos de cifra kex.

Falha ao ingressar no cluster.
Erro: "(3, 'Não foi possível encontrar o algoritmo de troca de chave correspondente.')"
Insira o endereço IP de uma máquina no cluster.

Solução

É necessário usar os valores padrão 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 os valores padrão, você pode executar o comando a partir de CLI **>** sshconfig **>** sshd na configuração passo a passo:

<#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
```

Confirmar as alterações

```
esa> commit

Please enter some comments describing your changes:

[]> Edit the SSHD values
```

Após a alteração, o dispositivo ingressa no cluster com êxito

Informações Relacionadas

[Configurar um cluster do ESA (Email Security Appliance)]

[Perguntas frequentes sobre ESA: quais são os requisitos para configurar um cluster?]

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.