

由于匹配密钥错误，对SEG加入集群失败进行故障排除

目录

简介

本文档介绍如何对无法加入现有集群的安全邮件网关(SEG)进行故障排除。

已预征

Cisco 建议您了解以下主题：

- 如何将设备加入集群（集中管理）。
- 所有ESA必须具有相同的AsyncOS版本（一直到修订版）。

要求

本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何命令的潜力

问题

将安全邮件网关(SEG)加入现有集群时出现问题。此问题提示连接出错，这是因为ESA缺少某些kex算法/加密算法。

无法加入集群。

错误为：“(3, '找不到匹配的密钥交换算法。')”

输入集群中计算机的IP地址。

解决方案

必须使用sshconfig的默认值

```
<#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
```

要应用默认值，可以在逐步设置时从CLI > sshconfig > sshd运行命令：

```
<#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,rijndael-cbc@lysator.liu.se
```

```
aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

```
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-
```

```
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
```

```
,
```

```
diffie-hellman-group1-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

提交更改

```
esa> commit
```

```
Please enter some comments describing your changes:
```

```
[ ]> Edit the SSHD values
```

更改后，设备成功加入集群

相关信息

[配置邮件安全设备\(ESA\)集群](#)

[ESA常见问题：设置集群有什么要求？](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。