

由於匹配金鑰錯誤，對SEG加入群集失敗進行故障排除

目錄

簡介

本文檔介紹如何對無法加入現有群集的安全電子郵件網關(SEG)進行故障排除。

預申請

思科建議您瞭解以下主題：

- 如何將裝置加入集群 (集中管理)。
- 所有ESA必須具有相同的AsyncOS版本 (一直到修訂版本)。

需求

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您已瞭解任何指令的潛力

問題

將安全電子郵件網關(SEG)加入現有群集時出現問題。此問題導致連線出錯，這是因為ESA丟失了一些kex演算法/密碼演算法。

無法加入群集。

錯誤為：「 (3, '找不到匹配的金鑰交換演算法。') 」

輸入集群中電腦的IP地址。

解決方案

必須使用sshconfig的預設值

```
<#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
```

要應用預設值，可以在逐步設定時從CLI > sshconfig > sshd運行命令：

```
<#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
```

更改後，裝置將成功加入群集

相關資訊

[配置郵件安全裝置\(ESA\)集群](#)

[ESA常見問題：設定群集的要求是什麼？](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。