一致キーエラーが原因でSEGをクラスタに参加できない場合のトラブルシューティング

内容

はじめに

このドキュメントでは、Secure Email Gateway(SEG)が既存のクラスタに参加できない場合のトラブルシューティング方法について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- アプライアンスをクラスタに参加させる方法（集中管理）
- すべての ESA で同じ AsyncOS バージョン（リビジョンまで）を持っていることが必須です。

要件

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。稼働中のネットワークで作業を行う場合は、コマンドの機能について十分に理解したうえで作業してください

問題

この問題は、Secure Email Gateway(SEG)を既存のクラスタに参加させるときに発生します。この問題により接続時にエラーが発生します。これは、ESAにkexアルゴリズム/暗号アルゴリズムの一部が欠落していることが原因です。

クラスターに参加できませんでした。
エラー：「(3, 'Could not find matching key exchange algorithm.')」
クラスタ内のマシンのIPアドレスを入力します。

解決方法

sshconfigにはデフォルト値を使用する必要があります

<#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
```

デフォルト値を適用するには、ステップバイステップのセットアップでCLI > sshconfig > sshdの順にコマンドを実行します。

<#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

変更を保存します。

```
esa> commit

Please enter some comments describing your changes:

[]> Edit the SSHD values
```

変更後、アプライアンスはクラスタに正常に参加します

関連情報

Eメールセキュリティアプライアンス(ESA)クラスタの設定

ESAに関するFAQ：クラスタをセットアップするための要件は何ですか。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。