키 일치 오류로 인해 SEG를 클러스터에 가입하지 못한 문제 해결

목차

소개

이 문서에서는 SEG(Secure Email Gateway)가 기존 클러스터에 조인할 수 없는 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 어플라이언스를 클러스터에 가입시키는 방법(중앙 집중식 관리).
- 모든 ESA의 AsyncOS 버전은 동일해야 합니다(개정판까지).

요구 사항

이 문서의 정보는 특정 랩 환경의 디바이스를 통해 생성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 모든 명령의 잠재력을 파악해야 합니다

문제

기존 클러스터에 SEG(Secure Email Gateway)를 조인할 때 문제가 발생합니다. 이 문제는 연결 시 오류가 발생했다는 것을 나타냅니다. ESA에서 일부 kex 알고리즘/암호 알고리즘이 누락되었기 때문입니다.

클러스터에 가입하지 못했습니다.
오류: "(3, '일치하는 키 교환 알고리즘을 찾을 수 없습니다.')"
클러스터에 있는 시스템의 IP 주소를 입력합니다.

솔루션

sshconfig에 대한 기본값을 사용해야 합니다.

<#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
```

기본값을 적용하려면 단계별 설정에서 CLI > sshconfig > sshd에서 명령을 실행할 수 있습니다.

<#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

변경 사항 커밋

```
esa> commit

Please enter some comments describing your changes:

[]> Edit the SSHD values
```

변경 후 어플라이언스는 클러스터에 성공적으로 조인합니다

관련 정보

[ESA(Email Security Appliance) 클러스터 구성]

[ESA FAQ: 클러스터 설정을 위한 요구 사항은 무엇입니까?]

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.