كيفية معالجة تكامل SMA و ESA بسبب فشل خوارزمية التبديل/التشفير الأساسية.

المحتويات

المقدمة
المشكلة
الحل
معلومات ذات صلة

المقدمة

يغطي هذا المستند كيفية معالجة حالات فشل تكامل "جهاز إدارة الأمان" (SMA) و"جهاز أمان البريد الإلكتروني" (ESA) التي ينتج عنها أخطاء: *(3، 'تعذر العثور على خوارزمية تبادل المفاتيح المطابقة.') أو "توصيل EOF غير متوقع"* وأعراض إضافية.

معلومات أساسية

اتصال SMA ب ESA أثناء الدمج لأول مرة، توفر SMA التشفير/خوارزميات تبادل المفاتيح التالية إلى ESA:

```
kex_algorithms string: diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-
sha1,diffie-hellman-group14-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
encryption_algorithms_client_to_server string: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-
cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client string: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-
cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

بعد تأسيس اتصال SMA و ESA، توفر SMA التشفير/خوارزميات تبادل المفاتيح التالية إلى ESA:

```
kex_algorithms string: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-
sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-
hellman-group14-sha1,diffie-hellman-group1-sha1
encryption_algorithms_client_to_server string [truncated]: aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-
poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-
cbc,arcfour,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client string [truncated]: aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-
poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-
cbc,arcfour,rijndael-cbc@lysator.liu.se
```

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المشكلة

توجد المشكلة عند دمج SMA في ESA من **واجهة المستخدم الرسومية (GUI) > جهاز الإدارة > الخدمات المركزية >**

أجهزة الأمان أو واجهة سطر الأوامر (CLI) > جهاز Applieconfig. ستسبب المشكلة خطأ في الاتصال، وذلك بسبب فقدان ESA لبعض خوارزميات kex/cipher.

```
('.Could not find matching key exchange algorithm' ,3) .1
.Error – Unexpected EOF on connect .2
```

الحل

لحل هذه المشكلة، يلزم إسترداد تكوين تشفير SSH ل ESA مرة أخرى إلى القيم الافتراضية التي تم توفيرها:

```
lab.esa.com> 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
```

الإنتاج من **ال sshd > sshconfig > CLI** على خطوة بخطوة setup:

```
[]> setup

Enter the Public Key Authentication Algorithms do you want to use
```

<[rsa1,ssh-dss,ssh-rsa]

Enter the Cipher Algorithms do you want to use
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-ripemd160@openssh.com,hmac-sha1-]
<[96,hmac-md5-96

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-group14-]
<[sha1,diffie-hellman-group1-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

معلومات ذات صلة

- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- الدعم التقني والمستندات - Cisco Systems
- أفضل الممارسات للحجر الصحي المركزي للفيروسات وتفشيها
- دليل شامل لإعداد عزل البريد العشوائي في ESA باستخدام SMA

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).