تشفير IM&P وفك تشفيره؛ مفاتح تشفير التوافق

المحتويات

المقدمة

يوضح هذا المستند كيفية تشفير مفاتح التشفير الذي تم إنشاؤه بواسطة IM&P وفك تشفيره للتكوين المشفر للتوافق.

المتطلبات الأساسية

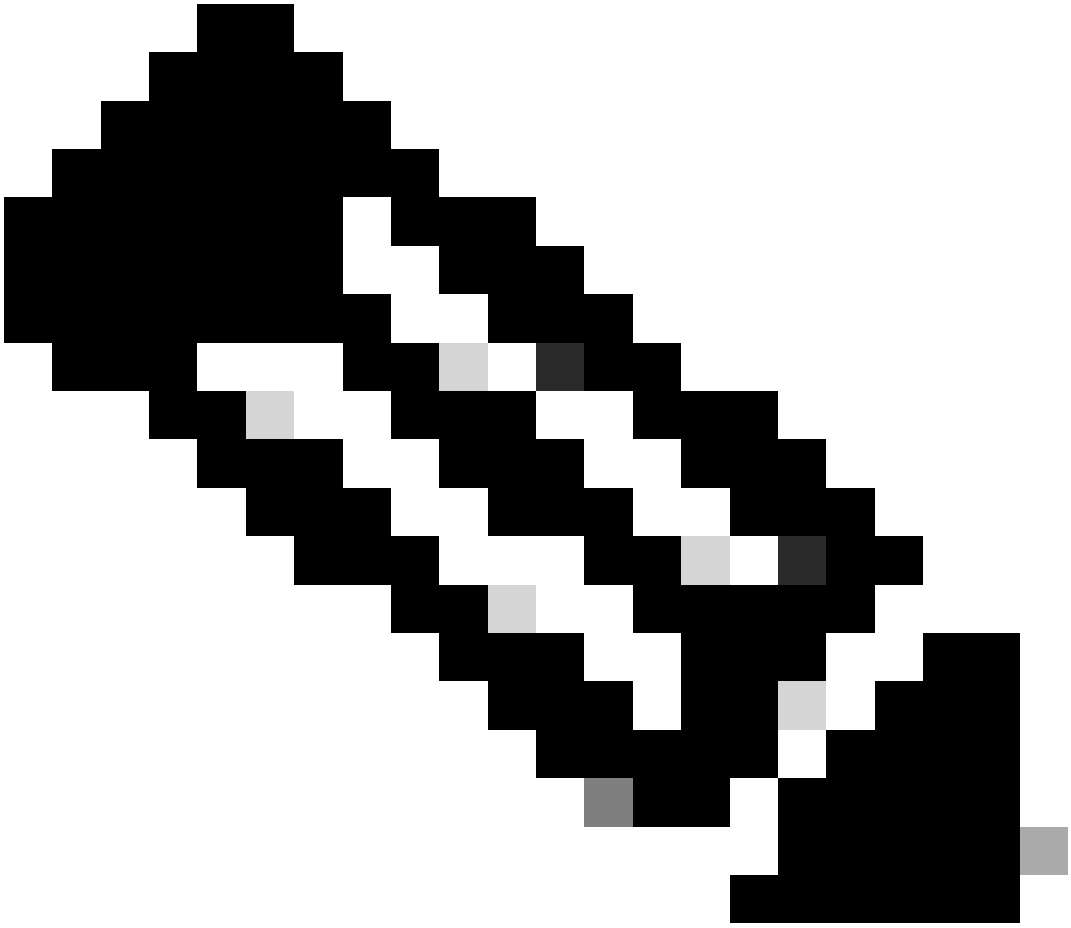
توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين برنامج أرشفة الرسائل
- OpenSSL

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- MacOS 15.5
- IM and Presence(IM&P)، الإصدار 15su2
- OpenSSL 3.3.6



ملاحظة: يمكن أن تختلف الأوامر الموضحة في هذا المستند بناءً على إصدار OpenSSL أو النظام الأساسي. الإنترنت مصدر جيد للعثور على الأشخاص الذين يتلاءمون مع بيئتك.

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.

معلومات أساسية

توفر ميزة "أرشفة الرسائل" حل التوافق الأساسي مع المراسلة الفورية. تتيح هذه الميزة للنظام لديك إمكانية التوافق مع اللوائح التي تتطلب تسجيل جميع حركات مرور المراسلة الفورية في شركتك. تتطلب العديد من الصناعات أن تلتزم الرسائل الفورية بنفس إرشادات التوافق التنظيمي كما هو الحال بالنسبة لجميع سجلات الأعمال الأخرى. للالتزام بهذه اللوائح، يجب أن يقوم النظام بتسجيل وأرشفة جميع سجلات الأعمال، ويجب أن تكون السجلات المؤرشفة قابلة للاسترداد.

للحصول على أمان إضافي، يمكنك تمكين قاعدة بيانات مشفرة لأرشفة الرسائل. عند تمكين هذا الخيار، تقوم خدمة المراسلة الفورية والحضور بتشفير رسائل فورية قبل أرشفتها في قاعدة البيانات الخارجية. مع هذا الخيار، يتم تشفير كل البيانات في قاعدة البيانات و الملفات التي تمت أرشفتها، إلا إذا كنت تمتلك مفاتيح التشفير.

يمكن تنزيل مفاتيح التشفير من خدمة المراسلة الفورية والحضور واستخدامه بالاقتران مع أي أداة تستخدمها لعرض البيانات لفك تشفير البيانات التي تمت أرشفتها.

تشفير / فك تشفير

1. افتح الوحدة الطرفية OpenSSL.
2. قم بإنشاء مفتاح خاص.

```
openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
```

3. إستخراج المفتاح العام من المفتاح الخاص.

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

4. عند هذه النقطة، لديك ملفان private_key.pem و public_key.pem.

- private_key.pem: يستخدم لفك تشفير المفتاح المشفر من IM&P.
- public_key.pem: هذا هو المفتاح الذي تشاركه مع خادم IM&P للسماح له بتشفير مفتاح AES و IV.

وبالإضافة إلى ذلك، يضيف خادم IM&P ترميز Base64 إلى مفتاح التشفير المشفر.

5. قم بتنزيل مفتاح التشفير من خادم IM&P، يرجى الرجوع إلى القسم تنزيل مفاتيح التشفير في دليل التوافق مع المراسلة الفورية لخدمة IM والحضور.
6. عند هذه النقطة، لديك 3 ملفات private_key.pem و public_key.pem و encrypted_key.pem.
7. في هذه الحالة Encrypted_key.pem يكون Based64 مرمز للبث الآمن.
8. فك ترميز المفتاح المشفر Base64.

```
base64 -D -i encrypted_key.pem -o encrypted_key.bin
```

يؤدي هذا إلى إزالة تشفير Base64 وينتج ملف مكون من 256 بايت تم تشفيره في الأصل باستخدام مفتاح RSA العام لديك.

9. قم بفك تشفير المفتاح المشفر باستخدام مفتاح RSA الخاص بك.

```
openssl pkeyutl -decrypt -inkey private_key.pem -in encrypted_key.bin -out decryptedkey.bin
```

يقوم هذا بفك تشفير مفتاح AES (K) و IV المستخدم لتشفير رسائل IM&P.

مثال على الملف الذي تم فك تشفيره:

المفتاح = 0ec39f2a22abf63d4452b932f12de

iv = 6683bb3d7e59e82e3fa9f42

10. فك تشفير الرسائل المشفرة AES.

```
openssl enc -aes-256-cbc -d -in encrypted.bin -out decrypted.txt -K <hex_key> -iv <hex_iv>
```

استكشاف الأخطاء وإصلاحها

من الأخطاء الشائعة عند محاولة فك تشفير الملف المشفر:

```
Public Key operation error 60630000:error:0200006C:rsa routines:rsa_ossl_private_decrypt:data greater t
```

يحدث هذا الخطأ عندما تحاول فك تشفير بيانات RSA التي تكون كبيرة جدا بالنسبة لحجم مفتاح RSA الخاص. يمكن ل RSA فك تشفير البيانات حتى حجم وحدات البت الخاصة به فقط. في حالتنا، يمكن لمفتاح RSA إصدار 2048 بت فك تشفير 256 بايت فقط.

إذا قمت بفحص ملف المفتاح المشفر الذي تم إنشاؤه بواسطة IM&P، tis 344 بايت. يمكنك فقط فك تشفير 256 بايت باستخدام مفتاحنا الخاص.

```
-rw-rw-rw-@ 1 testuser staff 344 Jun 5 13:10 encrypted_key.pem
```

كما تمت الإشارة مسبقا في هذا المستند، فإن المفتاح المشفر هو Base64 المشفر بالرسالة الآمنة، والذي يضيف وحدات البايت إلى حجم الملف.

بمجرد إزالة تشفير Base64، يكون لديك ملف بحجم 256 بايت، يمكن فك تشفيره بسهولة باستخدام مفتاحنا الخاص.

```
-rw-r--r-- 1 testuser staff 256 Jun 12 09:16 encrypted_key.bin
```

أفضل ممارسات الأمان

- قم بتخزين المفتاح الخاص (private_key.pem) بأمان.
- لا تشارك مفتاحك الخاص مع الآخرين أو قم بتحميله إلى أنظمة غير موثوق بها.
- تنظيف الملفات المؤقتة مثل decryptedkey.bin بعد فك التشفير.

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).