加密和解密IM&P合规性加密密钥

目录

简介

本文档介绍如何加密和解密IM&P为合规性加密配置生成的加密密钥。

先决条件

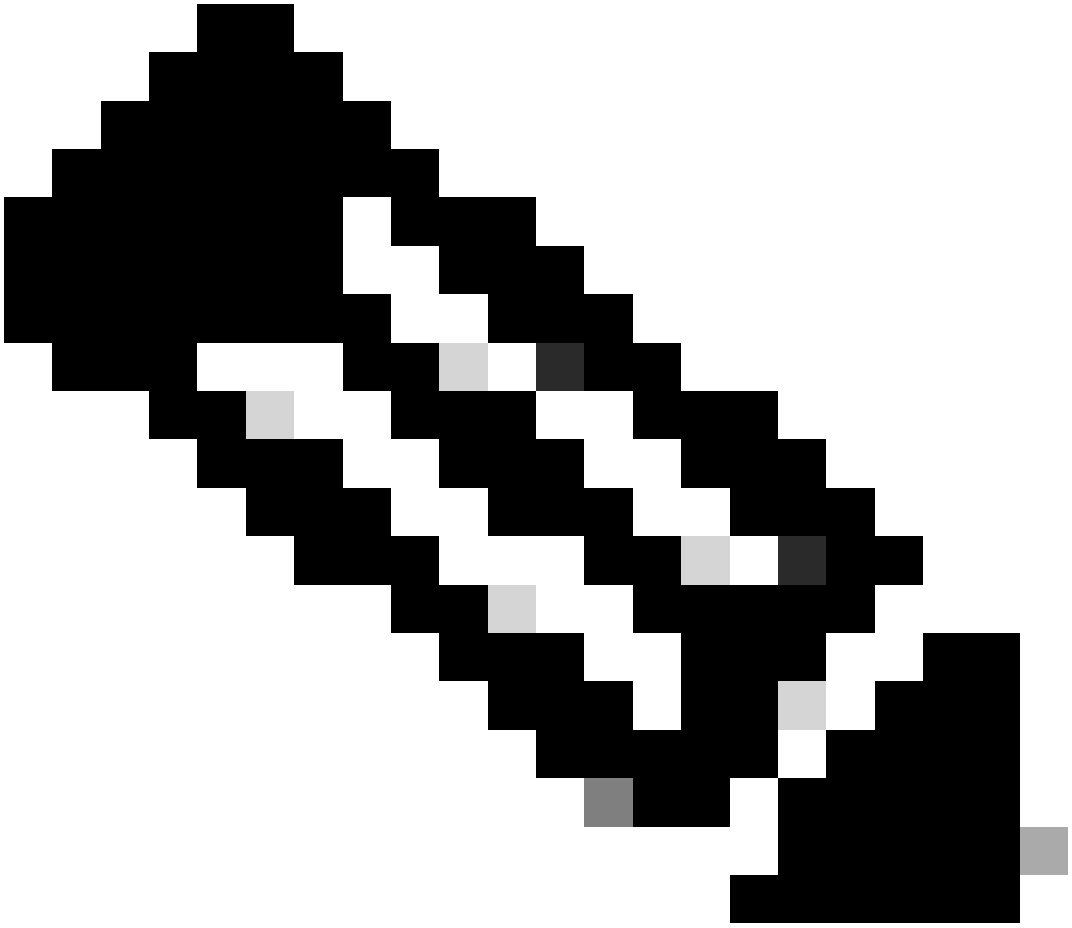
Cisco 建议您了解以下主题：

- 消息存档器配置
- OpenSSL

使用的组件

本文档中的信息基于以下软件版本：

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



注意：本文档中显示的命令可能因您的OpenSSL版本或平台而异。Internet是查找适合您环境的用户的良好来源。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

消息存档功能提供基本的即时消息合规性解决方案。此功能使您的系统符合要求记录公司所有即时消息流量的法规。许多行业要求即时消息遵守与其他所有业务记录相同的合规性准则。为遵守这些法规，您的系统必须记录并存档所有业务记录，而且必须可检索存档的记录。

为增强安全性，您可以为消息存档程序启用加密数据库。启用此选项后，即时消息和在线状态服务会在将即时消息存档到外部数据库之前对其进行加密。使用此选项，数据库中的所有数据都会被加密，并且除非您拥有加密密钥，否则您无法读取存档的即时消息。

加密密钥可以从IM and Presence Service下载，并与您用于查看数据以解密存档数据的任何工具配

合使用。

加密/解密

1. 打开OpenSSL终端。
2. 生成私钥。

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

3. 从私钥中提取公钥。

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

4. 此时，我们有2个文件private_key.pem和public_key.pem。

- private_key.pem:用于解密来自IM&P的加密密钥。
- public_key.pem:这是您与IM&P服务器共享的密钥，以允许它们加密AES密钥和IV。

此外，IM&P服务器向加密的加密密钥添加Base64编码。

5. 从IM&P服务器下载加密密钥，请参阅IM and Presence Service指南即时消息合规性指南中的下载加密密钥部分。
6. 此时，您有3个文件private_key.pem、public_key.pem和encrypted_key.pem。
7. 在本例中，encrypted_key.pem采用Based64编码以实现安全传输。
8. 解码Base64编码的加密密钥。

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

这将删除Base64编码，并生成最初使用公有RSA密钥加密的256字节文件。

9. 使用RSA私钥解密加密密钥。

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

这会解密用于IM&P消息加密的AES密钥(K)和IV。

已解密文件示例：

密钥= 0ec39f2a22abf63d4452b932f12de

iv = 6683bb3d7e59e82e3fa9f42

10. 解密AES加密的邮件。

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

故障排除

尝试解密加密文件时常见的错误是：

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

当您尝试RSA解密的数据对于RSA私钥的大小而言过大时，会发生此错误。RSA只能解密其模数大小的数据。在本例中，2048位RSA密钥只能解密256个字节。

如果检查IM&P生成的加密密钥文件，则其为34字节。您只能使用我们的私钥解密256 字节。

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

如本文档前面所述，加密密钥采用Base64编码，用于安全传输，这会向文件大小添加字节。

删除Base64编码后，您就有一个256字节的文件，可以使用私有密钥轻松解密。

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

安全最佳实践

- 安全地存储您的私钥(private_key.pem)。
- 请勿与他人共享您的私钥或将其上传到不受信任的系统。
- 在解密后清除临时文件，例如decryptedkey.bin。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。