加密和解密IM&P合規性加密金鑰

目錄

簡介

本文檔介紹如何加密和解密IM&P為合規性加密配置生成的加密金鑰。

必要條件

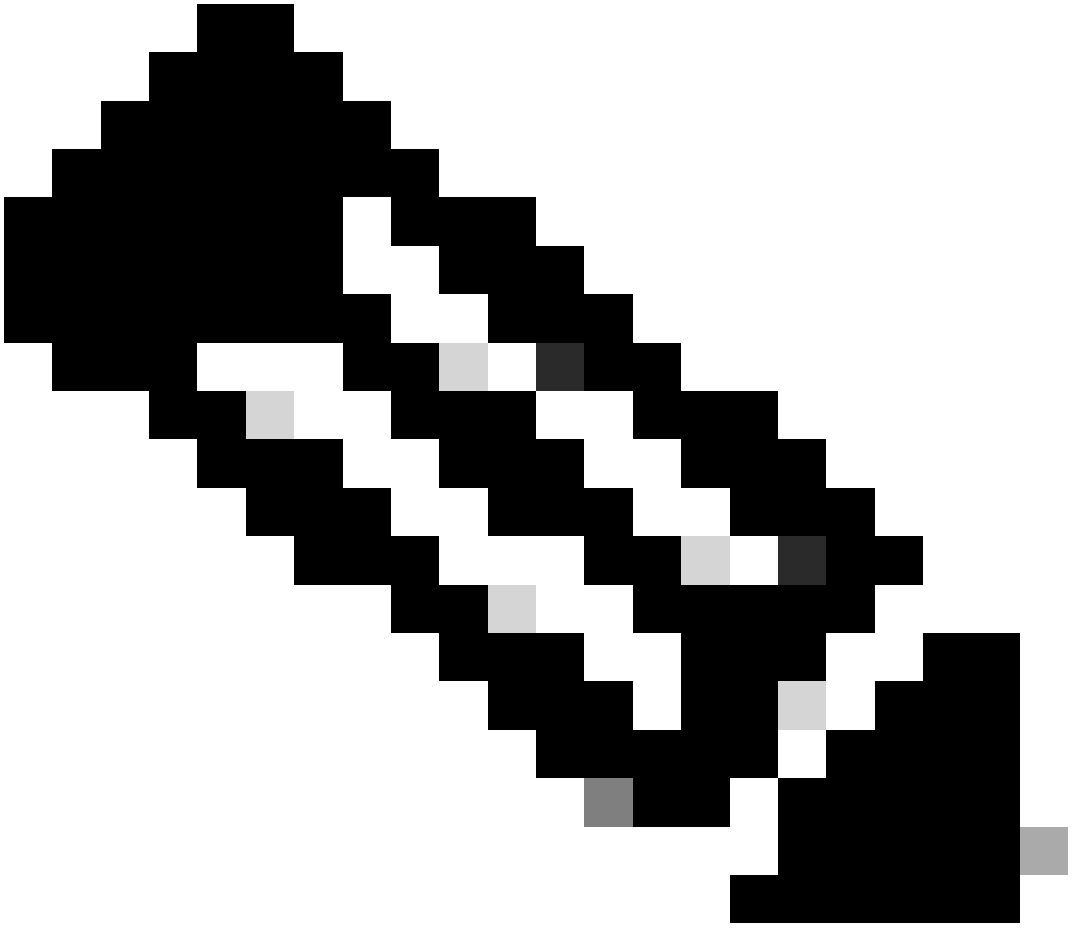
思科建議您瞭解以下主題：

- 消息存檔器配置
- OpenSSL

採用元件

本檔案中的資訊是根據以下軟體版本：

- MacOS 15.5
- 即時消息和線上狀態(IM&P)版本15su2
- OpenSSL 3.3.6



附註：本文檔中顯示的命令可能因您的OpenSSL版本或平台而異。Internet是查詢適合您環境的使用者的良好來源。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

消息存檔器功能提供了基本的IM合規性解決方案。此功能使您的系統符合要求記錄公司所有即時消息流量的法規。許多行業要求即時消息遵守與所有其他業務記錄相同的法規合規性准則。為遵守這些管理法規，您的系統必須記錄並歸檔所有業務記錄，而且必須可檢索歸檔的記錄。

為了增強安全性，您可以為消息存檔程式啟用加密資料庫。啟用此選項後，即時消息和線上狀態服務會在將即時消息存檔到外部資料庫之前對其進行加密。使用此選項，資料庫中的所有資料都將被加密，除非您擁有加密金鑰，否則您無法讀取存檔的即時消息。

加密金鑰可以從IM and Presence Service下載，並與您用來檢視資料以解密歸檔資料的任何工具結

合使用。

加密/解密

1. 開啟OpenSSL終端。
2. 生成私鑰。

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

3. 從私鑰中提取公鑰。

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

4. 此時，我們有2個檔案private_key.pem和public_key.pem。

- private_key.pem:用於解密來自IM&P的加密金鑰。
- public_key.pem:這是您與IM&P伺服器共用的金鑰，以允許它們加密AES金鑰和IV。

此外，IM&P伺服器會將Base64編碼新增到加密的加密金鑰中。

5. 從IM&P伺服器下載加密金鑰，請參閱IM and Presence服務的即時消息合規性指南指南中的下載加密金鑰部分。
6. 此時您有3個檔案private_key.pem、public_key.pem和encrypted_key.pem。
7. 在此案例中，encrypted_key.pem是Based64編碼的，用於安全傳輸。
8. 解碼Base64編碼的加密金鑰。

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

這將刪除Base64編碼，並生成最初使用公共RSA金鑰加密的256位元組檔案。

9. 使用RSA私鑰解密加密金鑰。

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

這將解密用於IM&P消息加密的AES金鑰(K)和IV。

解密檔案示例：

金鑰= 0ec39f2a22abf63d4452b932f12de

iv = 6683bb3d7e59e82e3fa9f42

10. 解密AES加密的郵件。

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

疑難排解

嘗試解密加密檔案時的常見錯誤為：

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

當您嘗試對資料進行RSA解密時，此錯誤會發生，因為對於RSA私鑰的大小而言，該資料過大。RSA只能對資料進行解密，直到達到其模數的大小。在本例中，2048位RSA金鑰只能解密256個位元組。

如果檢查IM&P產生的加密金鑰檔案，則為34bytes。您只能使用private key將256 位元組解密。

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

如本文檔前面所述，加密金鑰採用Base64編碼，用於安全傳輸，這會增加檔案大小的位元組。

刪除Base64編碼後，您就有一個256位元組的文件，可以使用private金鑰解密。

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

安全最佳實踐

- 安全地儲存您的私鑰(private_key.pem)。
- 請勿與他人共用您的私鑰或將其上傳到不受信任的系統。
- 解密後清理臨時檔案，如decryptedkey.bin。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。