Chiffrer et déchiffrer la clé de chiffrement de conformité IM&P

Table des matières

Introduction

Ce document décrit comment chiffrer et déchiffrer la clé de chiffrement générée par IM&P pour la configuration chiffrée de conformité.

Conditions préalables

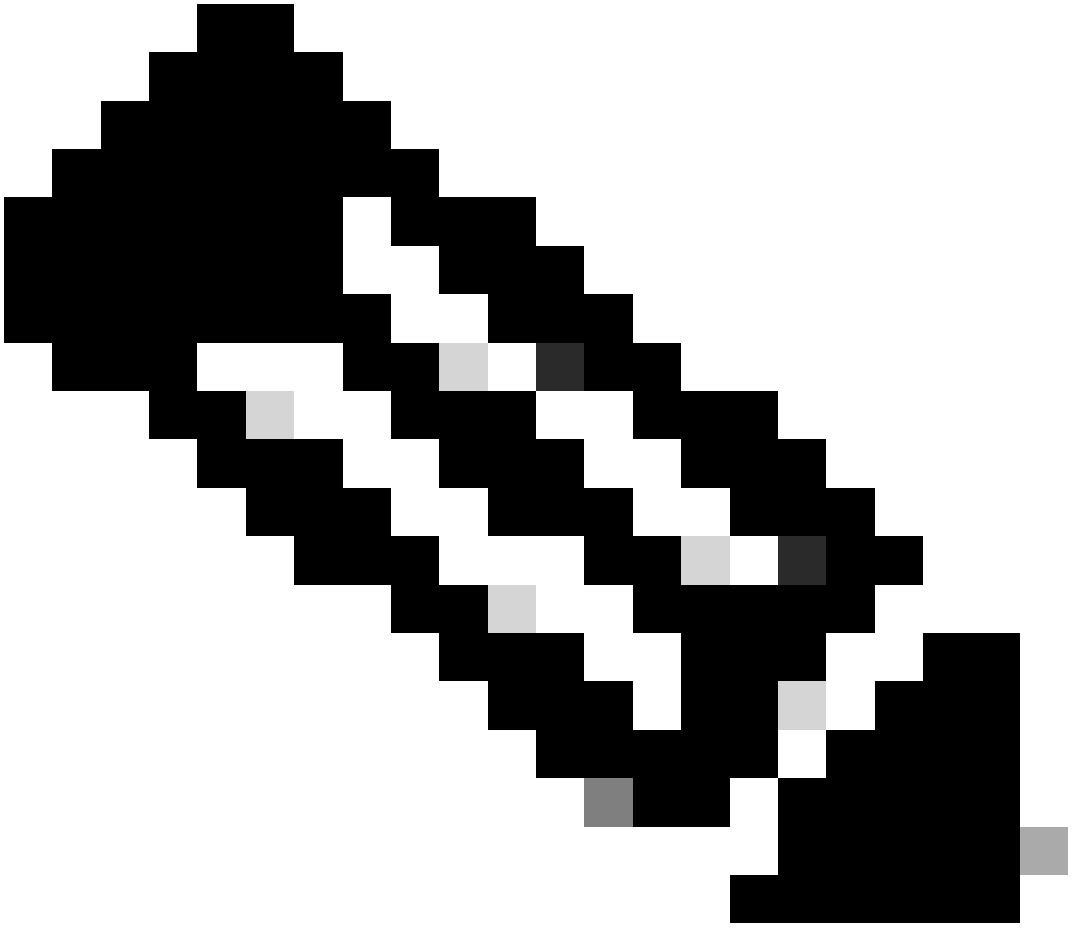
Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Message Archiver
- OpenSSL

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

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



Remarque : Les commandes présentées dans ce document peuvent varier en fonction de votre version ou de votre plate-forme OpenSSL. Internet est une bonne source pour trouver ceux qui correspondent à votre environnement.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

La fonctionnalité Message Archiver offre une solution de conformité de base pour la messagerie instantanée. Cette fonctionnalité permet à votre système de se conformer aux réglementations qui exigent la journalisation de tout le trafic de messagerie instantanée dans votre entreprise. De nombreux secteurs exigent que les messages instantanés respectent les mêmes directives de conformité que pour tous les autres documents professionnels. Pour se conformer à ces réglementations, votre système doit consigner et archiver tous les enregistrements de l'entreprise,

et les enregistrements archivés doivent pouvoir être récupérés.

Pour plus de sécurité, vous pouvez activer une base de données chiffrée pour l'outil Message Archiver. Lorsque cette option est activée, le service IM and Presence chiffre les messages instantanés avant de les archiver dans la base de données externe. Avec cette option, toutes les données de la base de données sont chiffrées et vous ne pouvez pas lire les messages instantanés archivés, sauf si vous possédez la clé de chiffrement.

La clé de cryptage peut être téléchargée à partir du service de messagerie instantanée et de présence et utilisée conjointement avec tout outil que vous utilisez pour afficher les données afin de décrypter les données archivées.

Chiffrer / Déchiffrer

1. Ouvrez votre terminal OpenSSL.
2. Générez une clé privée.

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

3. Extrayez la clé publique de la clé privée.

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

4. À ce stade, nous avons 2 fichiers private_key.pem et public_key.pem.

- private_key.pem : Utilisé pour déchiffrer la clé chiffrée de IM&P.
- public_key.pem : Il s'agit de la clé que vous partagez avec le serveur IM&P pour lui permettre de chiffrer la clé AES et IV.

En outre, le serveur IM&P ajoute le codage Base64 à la clé de cryptage cryptée.

5. Téléchargez la clé de cryptage à partir du serveur IM&P. Reportez-vous à la section Télécharger la clé de cryptage du guide Guide de conformité de la messagerie instantanée pour le service IM and Presence.
6. À ce stade, vous avez 3 fichiers private_key.pem, public_key.pem et encrypté_key.pem.
7. Dans ce cas, encryption_key.pem est encodé en Based64 pour une transmission sûre.
8. Décodez la clé chiffrée codée en Base64.

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

Ceci supprime le codage Base64 et produit un fichier de 256 octets qui a été chiffré à l'origine avec votre clé publique RSA.

9. Déchiffrez la clé chiffrée avec votre clé privée RSA.

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

Cette opération déchiffre la clé AES (K) et la clé IV utilisées pour le chiffrement des messages IM&P.

Exemple de fichier déchiffré :

clé = 0ec39f2a22abf63d4452b932f12de

iv = 6683bb3d7e59e82e3fa9f42

10. Déchiffrez les messages chiffrés AES.

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

Dépannage

Une erreur courante lors de la tentative de déchiffrement du fichier chiffré est la suivante :

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

Cette erreur se produit lorsque vous essayez de déchiffrer par RSA des données trop volumineuses pour la taille de votre clé privée RSA. RSA ne peut déchiffrer des données que jusqu'à la taille de son module. Dans notre cas, une clé RSA de 2 048 bits ne peut décrypter que 256 octets.

Si vous vérifiez le fichier de clé chiffrée généré par IM&P, il est de 344 octets. Vous ne pouvez déchiffrer que 256 octets avec votre clé privée.

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

Comme mentionné précédemment dans ce document, la clé chiffrée est codée en Base64 pour

une transmission sécurisée, ce qui ajoute des octets à la taille du fichier.

Une fois que nous supprimons le codage Base64, vous avez un fichier de 256 octets, facilement déchiffrable avec notre clé privée.

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

Meilleures pratiques de sécurité

- Stockez votre clé privée (private_key.pem) en toute sécurité.
- Ne partagez pas votre clé privée avec d'autres personnes et ne la téléchargez pas sur des systèmes non approuvés.
- Nettoyez les fichiers temporaires tels que decryptedkey.bin après le déchiffrement.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.