IM& 암호화 및 암호 해독;P 규정 준수 암호화 키

목차

소개

이 문서에서는 규정 준수 암호화 컨피그레이션을 위해 IM&P에서 생성한 암호화 키를 암호화하고 해독하는 방법에 대해 설명합니다.

사전 요구 사항

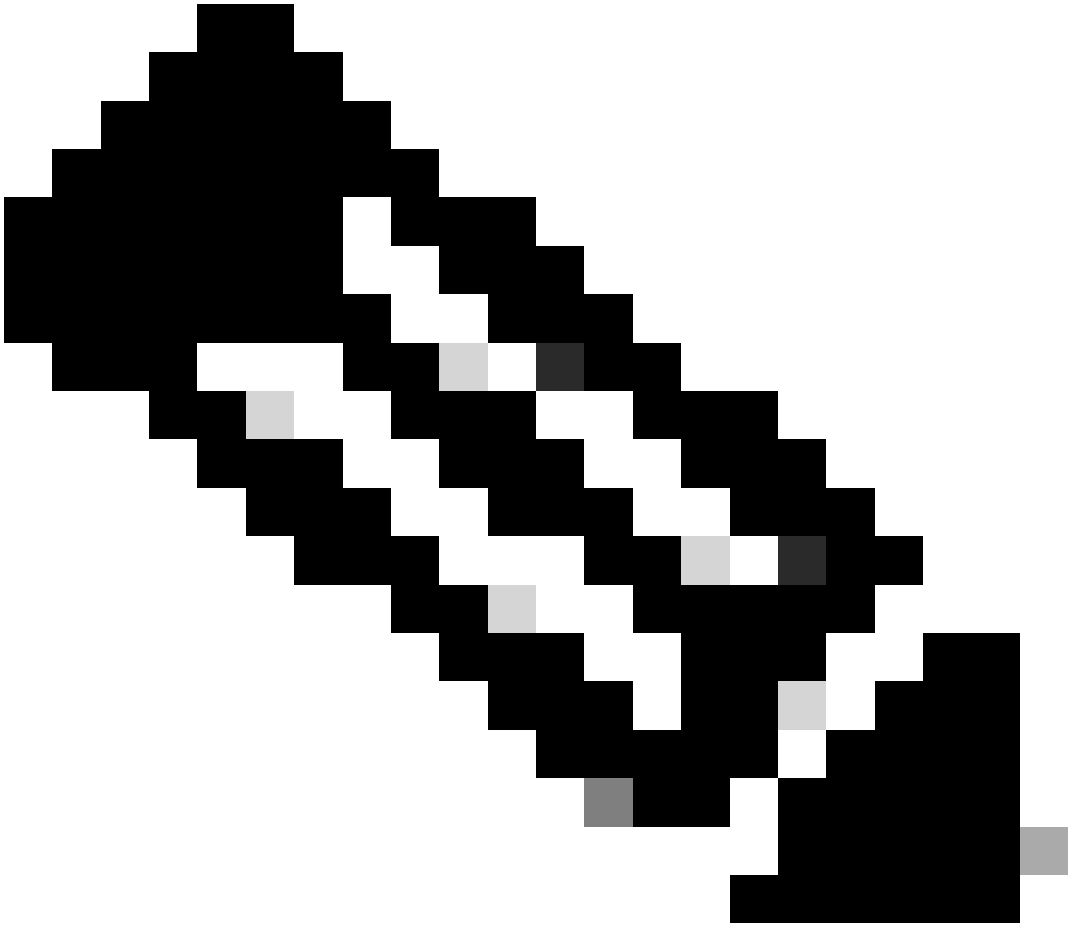
다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 메시지 아카이버 컨피그레이션
- OpenSSL

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

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



참고: 이 문서에 표시된 명령은 OpenSSL 버전 또는 플랫폼에 따라 달라질 수 있습니다. 인터넷은 당신의 환경에 맞는 사람들을 찾을 수 있는 좋은 원천입니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

메시지 아카이버 기능은 기본 IM 규정 준수 솔루션을 제공합니다. 이 기능을 사용하면 시스템에서 회사의 모든 인스턴트 메시징 트래픽을 기록해야 하는 규정을 준수할 수 있습니다. 많은 업계에서는 인스턴트 메시지가 다른 모든 비즈니스 기록과 동일한 규정 준수 지침을 준수해야 한다고 요구합니다. 이러한 규정을 준수하려면 시스템에서 모든 비즈니스 레코드를 기록하고 보관해야 하며, 보관된 레코드를 검색할 수 있어야 합니다.

보안을 강화하기 위해 메시지 아카이버에 대해 암호화된 데이터베이스를 활성화할 수 있습니다. 이 옵션이 활성화되면 IM and Presence Service는 IM을 외부 데이터베이스에 보관하기 전에 암호화합

니다. 이 옵션을 사용하면 데이터베이스의 모든 데이터가 암호화되며, 암호화 키를 소유하지 않는 한 보관된 IM을 읽을 수 없습니다.

IM and Presence Service에서 암호화 키를 다운로드하여 보관된 데이터를 해독하기 위해 데이터를 보는 데 사용하는 모든 툴과 함께 사용할 수 있습니다.

암호화/암호 해독

1. OpenSSL 터미널을 엽니다.
2. 개인 키를 생성합니다.

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

3. 개인 키에서 공개 키를 추출합니다.

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

4. 이 시점에서는 private_key.pem 및 public_key.pem 파일이 2개 있습니다.

- private_key.pem: IM&P에서 암호화된 키를 해독하는 데 사용됩니다.
- public_key.pem: 이 키는 IM&P 서버가 AES 키와 IV를 암호화할 수 있도록 IM&P 서버와 공유하는 키입니다.

또한 IM&P 서버는 암호화된 암호화 키에 Base64 인코딩을 추가합니다.

5. IM&P 서버에서 암호화 키를 다운로드합니다. IM and Presence Service에 대한 인스턴트 메시징 규정 준수 가이드의 암호화 키 다운로드 섹션을 참조하십시오.
6. 이 시점에는 private_key.pem, public_key.pem 및 encrypted_key.pem의 3개 파일이 있습니다.
7. 이 경우 encrypted_key.pem은 안전한 전송을 위해 Based64로 인코딩됩니다.
8. Base64 인코딩 암호화 키를 디코딩합니다.

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

이렇게 하면 Base64 인코딩이 제거되고 원래 공용 RSA 키로 암호화된 256바이트 파일이 생성됩니다.

9. RSA 개인 키로 암호화된 키를 해독합니다.

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

IM&P 메시지 암호화에 사용된 AES 키(K) 및 IV의 암호를 해독합니다.

암호 해독된 파일 예:

키 = 0ec39f2a22abf63d4452b932f12de

iv = 6683bb3d7e59e82e3fa9f42

10. AES 암호화 메시지를 해독합니다.

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

문제 해결

암호화된 파일을 해독하려고 할 때 흔히 발생하는 오류는 다음과 같습니다.

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

이 오류는 RSA 개인 키 크기에 비해 너무 큰 데이터를 RSA 암호 해독하려고 할 때 발생합니다. RSA는 해당 모듈러스 크기까지만 데이터를 암호 해독할 수 있습니다. 이 경우 2048비트 RSA 키는 256바이트만 해독할 수 있습니다.

IM&P에서 생성한 암호화된 키 파일을 확인하면 344바이트가 됩니다. 프라이빗 키로 256바이트를 해독할 수 있습니다.

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

이 문서에서 앞서 언급한 것처럼, 암호화된 키는 안전한 전송을 위해 인코딩된 Base64이며, 이는 파일 크기에 바이트를 추가합니다.

Base64 인코딩을 제거하면 256바이트 파일이 있으며, 프라이빗 키로 쉽게 해독할 수 있습니다.

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

보안 모범 사례

- 개인 키(private_key.pem)를 안전하게 저장합니다.
- 개인 키를 다른 사용자와 공유하거나 신뢰할 수 없는 시스템에 업로드하지 마십시오.
- 암호 해독 후 decryptedkey.bin과 같은 임시 파일을 정리합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.