SSL 인증서가 Cisco Email Security Appliance의 연결된 키로 서명되었는지 확인하는 방법

목차

질문

SSL 인증서가 Cisco Email Security Appliance의 연결된 키로 서명되었는지 확인하는 방법

환경: Cisco ESA(Email Security Appliance), 모든 버전의 AsyncOS

이 기술 자료 문서는 Cisco에서 유지 관리하거나 지원하지 않는 소프트웨어를 참조합니다. 이 정보는 귀하의 편의를 위해 제공됩니다. 자세한 내용은 소프트웨어 공급업체에 문의하십시오.

SSL 인증서 설치는 TLS 및 LDAP 보안 액세스를 통한 수신/전송 암호화를 위한 사전 요구 사항입니다.인증서는 CLI 명령 'certconfig'를 통해 설치됩니다. 설치하려는 인증서/키 쌍은 인증서에 서명한 키로 구성되어야 합니다.이를 준수하지 않으면 인증서/키 쌍을 설치하지 못합니다.

다음 단계는 인증서가 관련 키로 서명되었는지 확인하는 데 도움이 됩니다.'server.key'라는 파일에 개인 키가 있고 'server.cer'에 인증서가 있다고 가정합니다.

1. 인증서 및 키의 지수 필드가 동일한지 확인합니다.그렇지 않으면 키가 서명자가 아닙니다.다음 명령(openssl을 사용하는 표준 Unix 시스템에서 실행)은 이를 확인하는 데 도움이 됩니다.

```
$ openssl x509 -noout -text -in server.crt
$ openssl rsa -noout -text -in server.key
```

   인증서 및 키의 지수 필드가 동일한지 확인합니다.지수 키는 65537과 같아야 합니다.

2. 인증서와 키의 모듈러스에서 MD5 해시를 실행하여 동일한지 확인합니다.

```
$ openssl x509 -noout -modulus -in server.crt | openssl md5
$ openssl rsa -noout -modulus -in server.key | openssl md5
```

두 MD5 해시가 유사한 경우 키가 인증서에 서명했음을 확인할 수 있습니다.

관련 링크

http://www.modssl.org/docs/2.8/ssl_faq.html