如何驗證SSL證書是否已由思科郵件安全裝置上的關聯金鑰簽名？

目錄

問題

如何驗證SSL證書是否已由思科郵件安全裝置上的關聯金鑰簽名？

環境： 思科電子郵件安全裝置(ESA),AsyncOS的所有版本

本知識庫文章所參考的軟體不是思科維護或支援的。 此資訊出於方便而提供。 如需更多幫助，請與軟體供應商聯絡。

安裝SSL證書是通過TLS和LDAP安全訪問加密接收/傳送的先決條件。證書通過CLI命令「certconfig」安裝。 您打算安裝的證書/金鑰對必須包含已簽名證書的金鑰。如果不遵守此規則，將導致無法安裝證書/金鑰對。

下列步驟有助於驗證證書是否使用關聯金鑰簽名。假設您有一個名為「server.key」的檔案的私鑰和一個位於「server.cer」的證書。

1. 確保證書和金鑰的指數欄位相同。如果不是，則金鑰不是簽名者。以下命令（在任何帶有openssl的標準Unix電腦上運行）將幫助驗證這一點。

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

   確保證書和金鑰中的指數欄位相同。指數鍵應等於65537。

2. 對證書和金鑰的模數運行MD5雜湊以確保它們相同。

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

如果兩個MD5雜湊值相似，則可以確保金鑰已簽名證書。

相關連結

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