如何验证SSL证书由在思科电子邮件安全工具的相关的密钥签了字？

目录

问题

如何验证SSL证书由在思科电子邮件安全工具的相关的密钥签了字？

环境：思科电子邮件安全工具(ESA)， AsyncOS所有版本

此知识库文章参考没有维护也思科不支持的软件。 信息被提供作为礼貌为您的便利。 对于进一步协助，请联系软件供应商。

安装SSL证书是对加密接收/交付的一个前提通过TLS和LDAP安全访问。证书通过CLI命令‘certconfig’安装。您打算安装的证书/密钥对必须签署了证书的包括密钥。不符合此将导致失败对安装证书/密钥对。

以下步骤帮助验证证书是否签了字与相关的密钥。假设，您有一专用密钥在呼叫‘server.key’和在‘server.cer的’一证书的文件。

1. 确保证书和密钥的幂字段是相同的。如果这不是实际情形，则密钥不是签署人。以下命令(在任何标准的UNIX机器的运行有openssl的)将帮助验证此。

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

   确保证书的幂字段，并且密钥是相同的。幂密钥应该是相等的到65537。

2. 运行在证书的模数的一MD5哈希并且锁上保证他们是相同的。

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

如果两个MD5切细是类似的，则密钥签署证书的可以是确定的。

相关链接

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