Como verificar que o certificado SSL esteve assinado pela chave associada em uma ferramenta de segurança do email de Cisco?

Índice

[Pergunta](#)
[Links relacionados](#)

Pergunta

Como verificar que o certificado SSL esteve assinado pela chave associada em uma ferramenta de segurança do email de Cisco?

Ambiente: Cisco envia por correio eletrónico a ferramenta de segurança (ESA), todas as versões de AsyncOS

Este artigo da base de conhecimento provê o software que não é mantido nem é apoiado por Cisco. A informação é fornecida como uma cortesia para sua conveniência. Para a assistência adicional, contacte por favor o fornecedor de software.

Instalar Certificados SSL é uma condição prévia à recepção de criptografia/entrega através do TLS, e acesso seguro LDAP. Os Certificados são instalados através do comando CLI “certconfig”. O certificado/par de chaves que você pretende instalar deve compreender de uma chave que assine o certificado. Não seguir com o este conduzirá à falha instalar o certificado/par de chaves.

As seguintes etapas ajudam a verificar se o certificado esteve assinado com a chave associada. Supõe que você tem uma chave privada em um arquivo chamado “server.key” e um certificado em “server.cer”.

1. Certifique-se de que os campos do exponente do certificado e da chave são os mesmos. Se tal não for o caso, então a chave não é o signatário. Os comandos seguintes (corrida em alguma máquina padrão de Unix com OpenSSL) ajudarão a verificar este.

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

   Certifique-se que o campo do exponente no certificado e a chave são o mesmo. A chave do exponente deve ser igual a 65537.

2. Execute uma mistura MD5 no módulo do certificado e feche-a para assegurar-se de que sejam os mesmos.

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

Se os dois que o MD5 pica são similares, a seguir você pode ser assegurado que a chave assinou o certificado.

Links relacionados

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