¿Cómo verificar que el certificado SSL haya sido firmado por la clave asociada en un dispositivo de seguridad del correo electrónico de Cisco?

Contenido

Pregunta

¿Cómo verificar que el certificado SSL haya sido firmado por la clave asociada en un dispositivo de seguridad del correo electrónico de Cisco?

Entorno: Dispositivo de seguridad del correo electrónico de Cisco (ESA), todas las versiones de AsyncOS

Este artículo sobre Knowledge Base se refiere al software que no es mantenido ni es soportado por Cisco. La información se proporciona como cortesía para su conveniencia. Para la asistencia adicional, entre en contacto por favor al proveedor de software.

Instalar los Certificados SSL es un requisito previó a la recepción que cifra/salida vía TLS, y acceso seguro LDAP. Los Certificados están instalados vía el comando CLI “certconfig”. El certificado/el par clave que usted se prepone instalar debe comprender de una clave que ha firmado el certificado. La conformación con esto dará lugar al error instalar el certificado/el par clave.

Los pasos siguientes ayudan a verificar si el certificado se ha firmado con la clave asociada. Asuma que usted tiene una clave privada en un archivo llamado “server.key” y un certificado en “server.cer”.

1. Aseegurese que los campos del exponente del certificado y de la clave son lo mismo. En caso contrario, entonces la clave no es el firmante. Los siguientes comandos (funcionamiento en cualquier máquina estándar de Unix con el openssl) ayudarán a verificar esto.

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

   Aseegurese el campo del exponente en el certificado y la clave es lo mismo. La clave del exponente debe ser igual a 65537.

2. Funcione con un hash MD5 en el módulo del certificado y ciérrelo para asegurarse de que son lo mismo.

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

Si los dos que el MD5 desmenuza son similares, después usted puede ser confiado que la clave firmó el certificado.

Links relacionados

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