Comment vérifier que le certificat ssl a été signé par la clé associée sur une appliance de sécurité du courrier électronique de Cisco ?

Contenu

Question

Comment vérifier que le certificat ssl a été signé par la clé associée sur une appliance de sécurité du courrier électronique de Cisco ?

Environnement : Appliance de sécurité du courrier électronique de Cisco (ESA), toutes les versions d'AsyncOS

Cet article de la base de connaissances met en référence le logiciel qui n'est pas mis à jour ou est pris en charge par Cisco. Les informations sont données comme courtoisie pour votre commodité. Pour davantage d'assistance, contactez s'il vous plaît le fournisseur de logiciels.

Installer des Certificats SSL est une condition préalable à chiffrer la réception/livraison par l'intermédiaire de TLS, et accès sécurisé de LDAP. Des Certificats sont installés par l'intermédiaire de la commande « certconfig » CLI. Le certificat/paire de clés que vous avez l'intention d'installer doit comporter d'une clé qui a signé le certificat. L'acquiescement à ceci aura comme conséquence le manque d'installer le certificat/paire de clés.

Les étapes suivantes aident à vérifier si le certificat a été signé avec la clé associée. Supposez que vous avez une clé privée dans un fichier appelé « server.key » et un certificat dans « server.cer ».

1. Assurez-vous que les champs d'exposant du certificat et de la clé sont identiques. Si ce n'est pas le cas, alors la clé n'est pas le signataire. Les commandes suivantes (passage sur tout système Unix standard avec l'openssl) aideront à vérifier ceci.

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

   Assurez-vous que le champ d'exposant dans le certificat et la clé sont identique. La clé d'exposant devrait être égale à 65537.

2. Exécutez des informations parasites de MD5 sur le module du certificat et de la clé pour

s'assurer qu'ils sont identiques.

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

Si les deux MD5 hache sont semblables, alors vous pouvez être assurément que la clé a signé le certificat.

Liens connexes

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