Hoe kunt u controleren of het SSL-certificaat door de bijbehorende sleutel op een Cisco e-mail security applicatie is ondertekend?

Inhoud

vraag

Hoe kunt u controleren of het SSL-certificaat door de bijbehorende sleutel op een Cisco e-mail security applicatie is ondertekend?

Milieu: Cisco e-mail security applicatie (ESA), alle versies van AsyncOS

Deze Kennis Base artikel verwijst naar software die niet onderhouden of ondersteund wordt door Cisco. Deze informatie wordt ter beschikking gesteld als hoffelijkheid voor uw gemak. Voor verdere assistentie kunt u contact opnemen met de verkoper van de software.

Het installeren van SSL-certificaten is een voorwaarde voor het versleutelen van ontvangst/levering via TLS en LDAP veilige toegang. Certificaten worden geïnstalleerd via CLI opdracht 'certfig'. Het certificaat/de sleutel die u wilt installeren moet bestaan uit een sleutel die het certificaat heeft ondertekend. Wanneer u dit niet doet, bestaat er geen installatie van het certificaat of de sleutel.

De volgende stappen helpen controleren of het certificaat met de bijbehorende sleutel is ondertekend. Stel dat u een privé-sleutel hebt in een bestand genaamd 'server.key' en een certificaat in 'server.cer'.

1. Zorg ervoor dat de exponentiële velden van het certificaat en de toets hetzelfde zijn. Als dit niet het geval is, dan is de sleutel niet de ondertekenaar. De volgende opdrachten (uitgevoerd op een standaard Unix-machine met openssl) helpen dit te controleren.

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

   Zorg ervoor dat het veld EXP in certificaat en toets hetzelfde is. De exponentiële toets dient gelijk te zijn aan 65537.

2. Draai een MD5 hash op de modulus van zowel het certificaat als de sleutel om ervoor te zorgen dat ze hetzelfde zijn.

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

Als de twee MD5-hashes vergelijkbaar zijn, kunt u er zeker van zijn dat de sleutel met het certificaat is getekend.

Verwante links

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