Come verificare che il certificato SSL sia stato firmato dalla chiave associata su Cisco Email Security Appliance?

Sommario

Domanda

Come verificare che il certificato SSL sia stato firmato dalla chiave associata su Cisco Email Security Appliance?

Ambiente: Cisco Email Security Appliance (ESA), tutte le versioni di AsyncOS

Questo articolo della Knowledge Base fa riferimento a software non gestito o supportato da Cisco. Le informazioni sono fornite a titolo di cortesia. Per ulteriore assistenza, contattare il fornitore del software.

L'installazione dei certificati SSL è un prerequisito per la crittografia della ricezione/consegna tramite TLS e per l'accesso protetto LDAP. I certificati vengono installati tramite il comando CLI 'certconfig'. La coppia certificato/chiave che si desidera installare deve essere costituita da una chiave che ha firmato il certificato. Se non si rispetta questa impostazione, non sarà possibile installare la coppia certificato/chiave.

La procedura seguente consente di verificare se il certificato è stato firmato con la chiave associata. Si supponga di disporre di una chiave privata in un file denominato 'server.key' e di un certificato in 'server.cer'.

1. Verificare che i campi esponenti del certificato e della chiave siano uguali. In caso contrario, la chiave non è il firmatario. I comandi seguenti (eseguibili su qualsiasi computer Unix standard con openssl) consentono di verificare questa condizione.

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

   Verificare che il campo esponente nel certificato e nella chiave siano uguali. La chiave esponente deve essere uguale a 65537.

2. Eseguire un hash MD5 sul modulo del certificato e della chiave per verificare che siano uguali.

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

Se i due hash MD5 sono simili, è possibile assicurarsi che la chiave abbia firmato il certificato.

Collegamenti correlati

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