Wie kann überprüft werden, ob das SSL-Zertifikat vom entsprechenden Schlüssel auf einer Cisco E-Mail Security Appliance signiert wurde?

Inhalt

Frage

Wie kann überprüft werden, ob das SSL-Zertifikat vom entsprechenden Schlüssel auf einer Cisco E-Mail Security Appliance signiert wurde?

Umgebung: Cisco Email Security Appliance (ESA), alle Versionen von AsyncOS

Dieser Knowledge Base-Artikel bezieht sich auf Software, die nicht von Cisco verwaltet oder unterstützt wird. Die Informationen werden Ihnen zu Ihrer Zufriedenheit zur Verfügung gestellt. Wenden Sie sich für weitere Unterstützung an den Softwareanbieter.

Die Installation von SSL-Zertifikaten ist eine Voraussetzung für die Verschlüsselung von Empfang/Zustellung über TLS und sicheren LDAP-Zugriff. Zertifikate werden über den CLI-Befehl 'certconfig' installiert. Das Zertifikat-/Schlüsselpaar, das Sie installieren möchten, muss aus einem Schlüssel bestehen, der das Zertifikat signiert hat. Wenn Sie diese Anforderungen nicht erfüllen, wird die Installation des Zertifikats-/Schlüsselpaars fehlgeschlagen.

Die folgenden Schritte helfen zu überprüfen, ob das Zertifikat mit dem zugeordneten Schlüssel signiert wurde. Angenommen, Sie haben einen privaten Schlüssel in einer Datei namens 'server.key' und ein Zertifikat in 'server.cer'.

1. Stellen Sie sicher, dass die Exponent-Felder des Zertifikats und des Schlüssels identisch sind. Ist dies nicht der Fall, ist der Schlüssel nicht der Signaturgeber. Die folgenden Befehle (die auf jedem Unix-Standardcomputer mit openssl ausgeführt werden) helfen, dies zu überprüfen.

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

   Stellen Sie sicher, dass das Exponent-Feld in Zertifikat und Schlüssel identisch sind. Der Exponent-Schlüssel muss 65537 entsprechen.

2. Führen Sie einen MD5-Hash auf dem Modul des Zertifikats und des Schlüssels aus, um sicherzustellen, dass diese identisch sind.

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

Wenn die beiden MD5-Hashes ähnlich sind, können Sie sicher sein, dass der Schlüssel das Zertifikat signiert hat.

Verwandte Links

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