目次

質問

SSL 認証が Cisco E メール セキュリティ アプライアンスの関連するキーによって署名したことを確認する方法か。

環境： Cisco E メール セキュリティ アプライアンス（ESA）、AsyncOS のすべてのバージョン

このナレッジ ベース記事では、シスコによる保守およびサポートの対象でないソフトウェアを参照しています。 情報は、利便性のために無償で提供されています。 さらにサポートが必要な場合は、ソフトウェア ベンダーに連絡してください。

SSL 認証をインストールすることは TLS によって暗号化受信/配信への前提条件、および LDAP 安全なアクセスです。 認証は CLI コマンド「certconfig」によってインストールされています。 インストールするように意図する認証/キーペアはキーで構成する必要があります認証に署名した。 これに従わないことは認証/キーペアをインストールするために失敗に終わります。

次のステップは認証が関連するキーと署名したかどうか確かめるのを助けます。 「server.key」および「server.cer」の認証と呼ばれるファイルでプライベートキーがあると仮定して下さい。

1. 認証の指数フィールドおよびキーが同じであることを確かめて下さい。 これが事実ではない場合、キーは署名者ではないです。 次のコマンド（openssl が付いているあらゆる標準 UNIXマシンの実行）はこれの確認を助けます。

   認証の指数フィールドおよびキーが同じであることを確かめて下さい。 指数キーは 65537 と等しいはずです。

2. 認証の剰余の MD5 ハッシュを実行し、それらが同じであることを確認するためにキー入力して下さい。

キーが認証に署名した確実である場合もあれば MD5 がハッシュする 2 つが類似したである場合。

関連するリンク

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