サポートされている SSL 暗号の決定

この章では、サポートされている SSL 暗号を決定する方法について説明します。

SSL 暗号について

Cisco Application Centric Infrastructure（ACI）Representational State Transfer（REST）アプリケーションプログラミングインターフェイス（API）は、ソリューションがデビューした日から、HTTPS/SSL/TLS サポートがますます厳しくなる最近のバージョンへと進化を遂げました。このドキュメントは、Cisco ACI REST API での HTTPS、SSL、および TLS サポートの進化について説明し、クライアントが REST API を安全に利用するために必要なものに関するガイドを顧客に提供することを目的としています。

HTTPS は、Secure Socket Layers（SSL）または Transport Layer Security（TLS）のいずれかを利用して、HTTP セッションの安全な接続を形成するプロトコルです。SSL または TLS は、クライアントと HTTP サーバ間のトラフィックを暗号化するために使用されます。さらに、HTTPS をサポートするサーバーには、サーバーの信頼性を検証するためにクライアントが通常使用できる証明書があります。これは、サーバーで認証するクライアントの反対です。この場合、サーバーは「私は server_xyz です。それを証明する証明書はここにあります」と言っています。その後、クライアントはその証明書を利用して、サーバーが「server_xyz」であることを確認できます。

SSL/TLS には、SSL または TLS プロトコルの固有のセキュリティだけでなく、各プロトコルで使用可能なサポートされている暗号化方式も関係する、他の重要な側面があります。SSL は、SSLv1、SSLv2、SSLv3 の 3 回の反復を経て、現在ではすべて安全ではないと見なされています。TLS は、TLSv1、TLSv1.1、および TLSv1.2 の 3 つの反復を経ており、そのうち TLSv1.1 と TLSv1.2 のみが「安全」と見なされています。理想的には、クライアントは利用可能な最高の TLS バージョンを利用し、サーバーは TLSv1.1 と TLSv1.2 のみをサポートする必要があります。ただし、ほとんどのサーバは、古いクライアントに対して TLSv1 を保持する必要があります。

ほぼすべての最新のブラウザで、TLSv1.1 と TLSv1.2 の両方をサポートしています。ただし、HTTPS を使用するクライアントはブラウザではない場合があります。クライアントは、Web

サーバーと通信し、HTTPS/TLS をネゴシエートする必要がある Java アプリケーションまたは Python スクリプトである場合があります。このような状況では、何をどこでサポートするかという問題がより重要になります。

CLI を使用してサポートされている SSL 暗号を判別する

始める前に

このセクションでは、CLI を使用して、サポートされている SSL 暗号を判別する方法について説明します。

ステップ 1 次に示されているように、OpenSSL 環境でサポートされている暗号を取得します。

例：

```
openssl ciphers 'ALL:eNULL'
```

ステップ 2 次に示されているように、sed またはその他のツールを使用して暗号を分離します。

例：

```
openssl ciphers 'ALL:eNULL' |  sed -e 's/:/\n/g'
```

ステップ 3 次のように、暗号をループし、APIC をポーリングして、サポートされている暗号を確認します。

例：

```
openssl s_client -cipher '<some cipher to test>' -connect <apic ipaddress>:<ssl port, usually 443>
```

次の暗号の例を参照してください。

例：

```
openssl s_client -cipher 'ECDHE-ECDSA-AES128-GCM-SHA256' -connect 10.1.1.14:443
```

（注）　応答に CONNECTED が含まれている場合、その暗号はサポートされています。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。