Cisco Business DashboardおよびDNS検証による証明書の暗号化の使用方法

目的

このドキュメントでは、コマンドラインインターフェイス(CLI)を使用して証明書を暗号化し、Cisco Business Dashboardにインストールする方法について説明します。 証明書の管理に関する一般的な情報が必要な場合は、「Cisco Business Dashboardの証明書の管理」を参照してください。

概要

暗号化とは、自動的なプロセスを使用して、無料のドメイン検証(DV)SSL証明書を公開する認証局です。Encryptは、Webサーバの署名付き証明書を取得するための簡単にアクセス可能なメカニズムを提供し、エンドユーザが正しいサービスにアクセスしているという安心感を与えます。暗号化の詳細については、暗号化のLet's Encrypt Webサイトを参照してください。

Cisco Business Dashboardで証明書を暗号化する方法は簡単です。Cisco Business Dashboardには、証明書をWebサーバで使用できるようにするだけでなく、証明書のインストールに関する特別な要件もありますが、提供されているコマンドラインツールを使用して、証明書の発行とインストールを自動化することも可能です。

証明書を自動的に発行して更新するには、ダッシュボードWebサーバにインターネットからアクセスできる必要があります。そうでない場合は、手動プロセスを使用して証明書を簡単に取得し、コマンドラインツールを使用してインストールできます。このドキュメントの残りの部分では、証明書を発行し、ダッシュボードにインストールするプロセスについて説明します。

ダッシュボードWebサーバが標準ポートTCP/80およびTCP/443でインターネットから到達可能な場合、証明書管理とインストールプロセスを自動化できます。詳細はLet's Encrypt for Cisco Business Dashboardを参照してください。

手順 1

最初のステップは、ACMEプロトコル証明書を使用するソフトウェアを取得することです。この例では、certbotクライアントを使用していますが、他にも多くのオプションがあります。

certbotクライアントを入手するには、UnixライクなOS（Linux、macOSなど）を実行しているダッシュボードまたは別のホストを使用し、certbotクライアントの指示に従ってクライアントをインストールします。このページのドロップダウンメニューで、[ソフトウェア]に[上記なし]を選択し、システムに適したOSを選択します。

この記事では、青色のセクションがプロンプトとCLIからの出力であることに注意してください。白いテキストにリストされています。dashboard.example.com、pnpserver.example.com、user@example.comなどの緑色のコマンドは、環境に適したDNS名に置き換える必要があります。

Cisco Business Dashboardサーバにcertbotクライアントをインストールするには、次のコマンドを使用します。

```
cbd:$sudo apt update cbd:$sudo apt install software-properties-common cbd:$sudo add-apt-
```

```
repository ppa:certbot/certbot cbd:$sudo apt update cbd:$sudo apt install certbot
```

手順 2

証明書に関連付けられたすべてのファイルを含む作業ディレクトリを作成します。これらのファイルには、証明書の秘密キーや*Let's Encryptサービスのアカウントの詳細などの機密情報が含まれていることに注意して*ください。certbotクライアントは適切に制限されたアクセス許可を持つファイルを作成しますが、ホストと使用されているアカウントが許可されたスタッフのみにアクセスするように制限されていることを確認する必要があります。

ダッシュボードにディレクトリを作成するには、次のコマンドを入力します。

```
cbd:$mkdir certbot cbd:/certbot $cd certbot
```

手順 3

次のコマンドを使用して証明書を要求します。

```
cbd:/certbot$certbot certonly –manual –preferred-challenge dns -d dashboard.example.com -d
pnpserver.example.com
–logs-dir–config-dir–work-dir–deploy-hook "cat /certbot/live/dashboard.example.com
/fullchain.pem /etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem;/usr/bin/cisco-business-
dashboard importcert -t pem -k /certbot/live/dashboard.example.com /privkey.pem -c
/tmp/cbdchain.pem"
```

このコマンドは、「*Let's Encrypt*」*サービスに対して*、リストされている各名前に対してDNS TXTレコードを作成するよう求めるプロンプトを表示し、ホスト名の所有権を検証するように指示します。TXTレコードが作成されたら、「*Let's Encrypt*」*サービスでレコードが存在*することを確認し、証明書を発行します。最後に、cisco-business-dashboardユーティリティを使用して、証明書がダッシュボードに適用されます。

コマンドのパラメータは、次の理由で必要になります。

ceronly	証明書を要求し、ファイルをダウンロードします。インストールしないでくだ ます。その結果、certbotクライアントは証明書を自動的にインストールできま
--手動	Let's Encryptサービスで自動的に認証*を試みないで*ください。ユーザと対話形式
—preferred-challenges dns	DNS TXTレコードを使用して認証します。
-d dashboard.example.com -d pnpserver.example.com	証明書に含める必要があるFQDN。リストされた最初の名前が証明書の[Commo pnpserver.<ドメイン>名は、DNS検出を実行するときにネットワークプラグア を参照してください。
—logs-dir。 —config-dir —work-dir。	処理中に作成されたすべての作業ファイルに対して、現在のディレクトリを使
—deploy-hook "..."	*Let's Encryptサービスから受信した秘密キーと証明書チェーンを*cisco-business ードされたのと同じ方法でダッシュボードアプリケーションにロードします。 証明書チェーンをアンカーするルート証明書も、ここで証明書ファイルに追加

—deploy-hookオプションを使用した証明書の自動インストールは、certbotクライアントがダッシュボードサーバで実行されている場合にのみ可能です。certbotクライアントが別のコンピュータで実行されている場合は、秘密キーとフルチェーン証明書ファイルをダッシュボードサーバにコピーし、次のコマンドを使用してインストールする必要があります。

-cat <fullchain certificate file> /etc/ssl/certs/DST_Root_CA_X3.pem >/tmp/cbdchain.pem

cisco-business-dashboard importcert -t pem -k <秘密キーファイル> -c /tmp/cbdchain.pem

手順 4

certbotクライアントによって生成される手順に従って、証明書を作成するプロセスを実行します。

```
cbd:/certbot$certbot certonly –manual –preferred-challenge dns -d dashboard.example.com -d
pnpserver.example.com
–logs-dir–config-dir–work-dir–deploy-hook "cat /certbot/live/dashboard.example.com
/fullchain.pem /etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem;/usr/bin/cisco-business-
dashboard importcert -t pem -k /certbot/live/dashboard.example.com /privkey.pem -c
tmp/cbdchain.pem"
/home/cisco/certbot/letsencrypt.log
```

手順 5

キャンセルする電子メールアドレスまたは**Cを**入力してください。

```
c:user@example.com
HTTPS(1):acme-v02.api.letsencrypt.org
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

手順 6

同意する**にはAを**、キャンセルする**にはCを**入力してください。

```
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf
ACME
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
AC
(A)gree/(C)A
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

ステップ7

[はい]に**はYを**、[いいえ]に**はNを**入力します。

```
Let's EncryptFoundation

webEFF
[]Y[]N
(Y)es/(N)o:Y


dashboard.example.comdns-01
pnpserver.example.comdns-01
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

手順 8

[はい]に**はYを**、[いいえ]に**はNを**入力します。

```
IP
.Certbot

IP
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[]Y[]N
(Y)es/(N)o:Y
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DNS TXT
_acme-challenge.dashboard.example.com
3AzDTqNGXb8kSkhqXXYWE2iZrFAVCGT2B8oZNGyBwhc
```

手順 9

dashboard.example.comホスト名の所有権を検証するDNS TXTレコードをDNSインフラストラクチャに作成する必要があります。これを行うために必要な手順は、このドキュメントの範囲外であり、使用されているDNSプロバイダーによって異なります。作成したら、DigなどのDNSクエリツールを使用して、レコードが使用可能であることを確認します。

DNSチャレンジプロセスは、特定のDNSプロバイダーに対して自動化できます。詳細はDNSプラグインを参照してください。

キーボードで**Enter**キーを押します。

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Enter
```

手順 10

同様のCLI出力が表示されます。証明書に含める各名前の追加のTXTレコードを作成して確認します。certbotコマンドで指定した名前ごとに、手順9を繰り返します。

キーボードで**Enter**キーを押します。

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DNS TXT
_acme-challenge.pnpserver.example.com
Txruc89x8dVaHmLHJII0oA2ILmIY83XYl13yYakjNuc

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Enter
```

手順 11

証明書が発行され、ファイルシステムの*live*サブディレクトリに保存されます。

```
…

crontab
deploy-hookcat /certbot/live/dashboard.example.com/fullchain.pem
```

```
/etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem/usr/bin/cisco-business-dashboard
importcert -t pem -k /certbot/live/dashboard.example.com/privkey.pem -c /tmp/cbdchain.pem

-
/home/cisco/certbot/live/dashboard.example.com/fullchain.pem

/home/cisco/certbot/live/dashboard.example.com/privkey.pem
2020-11-11
certbot
*all*
certbot renew
– Certbot
/home/cisco/certbot

Certbot

- Certbot
ISRG/https://letsencrypt.org/donate
EFFhttps://eff.org/donate-le
```

ステップ 12

次のコマンドを入力します。

```
cbd:/certbot$cd live/dashboard.example.com/ cbd:/certbot/live/dashboard.example.com$ls
cert.pem chain.pem fullchain.pem privkey.pem README
```

証明書を含むディレクトリには制限付き権限があるため、シスコユーザだけがファイルを表示できます。特に*privkey.pem*ファイルは機密性が高く、このファイルへのアクセスは権限のあるユーザのみに制限する必要があります。

新しい証明書を使用してダッシュボードが実行されます。証明書を作成するときに指定した名前をアドレスバーに入力してWebブラウザでダッシュボードのユーザーインターフェイス(UI)を開くと、接続が信頼され、セキュリティ保護されていることをWebブラウザが示します。

Let's Encryptで発行された証明書*の有効期間は比較的短*く、現在90日です。証明書が有効であることを確認するには、90日前に上記のプロセスを繰り返す必要があります。

certbotクライアントの使用方法の詳細については、certbotのドキュメントページを参照してください。