Cisco Business Dashboardで証明書を暗号化する方法

目的

このドキュメントでは、*Let's Encrypt証明書を取得し、Cisco Business Dashboardにインストールし*、コマンドラインインターフェイス(CLI)を使用して自動更新を設定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。

このドキュメントで説明するプロセスは、Cisco Business Dashboardバージョン2.2.2以降で自動化されています。詳細については、『 アドミニストレーションガイド』の「システム」>「証明書の管理」セクションを参照してください。

概要

*Encryptは、自動化されたプロセスを使用*して、無料のドメイン検証(DV)セキュアソケットレイヤ(SSL)証明書を公開する認証局です。*Encryptは、Webサーバの署名済み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。詳細については、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。このドキュメントの残りの部分では、証明書を発行し、証明書の更新を自動化するプロセスについて説明します。

このドキュメントでは、HTTPの課題を使用してドメインの所有権を検証します。これには、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である必要があります。Webサーバがインターネットから到達可能でない場合は、代わりにDNSチャレンジを使用することを検討してください。詳細については、「Let's Encrypt for Cisco Business Dashboard with DNS」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。

手順 2

証明書の更新を自動化するには、certbotクライアントをダッシュボードにインストールする必要があります。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。

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。

```
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 3

次に、ホスト名の所有権を確認するために必要なチャレンジファイルをホストするようにダッシュボードWebサーバを設定する必要があります。そのためには、これらのファイルのディレクトリを作成し、Webサーバ設定ファイルを更新します。次に、ダッシュボードアプリケーションを再起動して、変更を有効にします。次のコマンドを使用します。

```
cbd:$sudo mkdir /usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd:$sudo chmod 755
/usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd:$sudo bash -c 'cat >
/var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf' << EOF
# certbot location /.well-known/acme-challenge {
root/usr/lib/ciscobusiness/dashboard/www/letsencrypt;
}
EOF
cbd:$ cbd:$sudo chown cbd:cbd /var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf
cbd:$sudo chmod 640 /var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf cbd:$cisco-
business-dashboard stop cbd:$cisco-business-dashboard start
```

手順 4

次のコマンドを使用して証明書を要求します。

```
cbd:$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com —deploy-hook "cat /etc/letsencrypt/live/
dashboard.com /fullchain.pem > /tmp/cbdchain.pem;/usr/bin/cisco-business-dashboard importcert -t
pem -k /etc/letsencrypt/live/dashboard.example.com /privkey.pem -c /tmp/cbdchain.pem
```

このコマンドは、各*名前でホストされるWebサービスに接続*して提供されるホスト名の所有権を検証するために、暗号化サービスに指示します。これは、ダッシュボードWebサービスがインターネットからアクセス可能で、ポート80および443でホストされている必要があることを意味します。ダッシュボード管理ユーザーインターフェイス(UI)の[システム(System)] > [プラットフォーム設定(Platform Settings)] > [Webサーバ(Web Server)]ページのアクセス制御 詳細については、『Cisco Business Dashboard Administration Guide』を参照してください。

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
—webroot -w..	ダッシュボードWebサーバからアクセスできるように、上記で作成したディレ
-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[Comm 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。
—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

手順 5

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:$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com —deploy-hook "cat /etc/letsencrypt/live/
dashboard.com /fullchain.pem > /tmp/cbdchain.pem;/usr/bin/cisco-business-dashboard importcert -t
pem -k /etc/letsencrypt/live/dashboard.example.com /privkey.pem -c /tmp/cbdchain.pem"
/var/log/letsencrypt/letsencrypt.log
WebRoot
```

手順 6

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
```

ステップ7

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
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)A
```

手順 8

[はい]に**はY**を、[いいえ]に**はN**を入力します。

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Let's Encrypt

webEFF
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o:Y
```

手順 9

証明書が発行され、ファイルシステムの*/etc/letsencrypt/live*サブディレクトリにあります。

```
dashboard.example.comhttp-01
pnpserver.example.comhttp-01
webroot/usr/lib/ciscobusiness/dashboard/www/letsencrypt
…

deploy-hookcat /etc/letsencrypt/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 /etc/letsencrypt/live/dashboard.example -c /tmp/cbdchain.pem
```

```
-
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem

/etc/letsencrypt/live/dashboard.example.com/privkey.pem
2020-10-29
certbot
*all*
certbot renew
– Certbot
/etc/letsencrypt

Certbot

- Certbot
ISRG/https://letsencrypt.org/donate
EFFhttps://eff.org/donate-le
cbd:$ sudo ls /etc/letsencrypt/live/dashboard.example.com
/ cert.pem chain.pem fullchain.pem privkey.pem README
cbd:$
```

証明書を含むディレクトリには制限されたアクセス許可があるため、ルート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。

手順 10

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。Ubuntu Linux用のcertbotパッケージは、証明書の有効性を1日2回確認し、有効期限が近づいている場合は証明書を更新するように構成されているため、証明書を最新の状態に保つ必要はありません。定期的なチェックが正しく行われていることを確認するには、最初に証明書を作成してから12時間以上待ってから、certbotログファイルで次のようなメッセージを確認します。 `cbd:$ sudo tail`

```
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52,783:DEBUG:certbot.main:certbot version:0.31.0
2020-07-31 16:50:52,784:DEBUG:certbot.main['-q']
2020-07-31 16:50:52,785:DEBUG:certbot.main
(PluginEntryPoint#manual,
PluginEntryPoint#null,PluginEntryPoint#standalone,PluginEntryPoint#webroot)
2020-07-31 16:50:52,793:DEBUG:certbot.log30
2020-07-31 16:50:52,793:INFO:certbot.log
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52,802:DEBUG:certbot.plugins.selection:
<certbot.cli
_Default object at 0x7f1152969240>installer <certbot.cli
_0x7f1152969240>
2020-07-31 16:50:52,811:INFO:certbot.renewal
2020-07-31 16:50:52,812:DEBUG:certbot.plugins.selection:Requested authenticator
webrootinstaller
2020-07-31 16:50:52,812:DEBUG:certbot.renewal:no renewal failures
```

証明書の有効期限が30日以内に経過すると、certbotクライアントは証明書を更新し、更新された証明書をダッシュボードアプリケーションに自動的に適用します。

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。