証明書のオプション

証明書のオプション

この記事では、自己ホスト型のBitwardenインスタンスに利用可能な証明書のオプションを定義しています。
インストール中に証明書のオプションを選択します。

> **Note**
> この記事の情報は、Bitwarden統一自己ホスト型のデプロイメントには適用されないかもしれません。

Let's Encryptで証明書を生成します

Let's Encrypt は、あらゆるドメインに対して信頼できる SSL 証明書を無料で発行する認証局 (CA) です。
Bitwardenのインストールスクリプトは、Let's
EncryptとCertbotを使用してあなたのドメインのための信頼できるSSL証明書を生成するオプションを提供します。

証明書の更新チェックは、Bitwardenが再起動するたびに行われます。Let's Encryptを使用するには、
証明書の有効期限のリマインダーのためにメールアドレスを入力する必要があります。

Let's Encryptを使用するには、マシンでポート80と443を開放する必要があります。

Let's Encrypt証明書を手動で更新します

あなたがBitwardenサーバーのドメイン名を変更する場合、生成された証明書を手動で更新する必要があります。
次のコマンドを実行してバックアップを作成し、証明書を更新し、Bitwardenを再構築します:

🐧🍎バッシュ

```Bash
./bitwarden.sh stop

mv ./bwdata/letsencrypt ./bwdata/letsencrypt_backup

mkdir ./bwdata/letsencrypt

chown -R bitwarden:bitwarden ./bwdata/letsencrypt

chmod -R 740 ./bwdata/letsencrypt

docker pull certbot/certbot

docker run -i --rm --name certbot -p 443:443 -p 80:80 -v <Full Path from / >/bwdata/letsencrypt:/et
c/letsencrypt/ certbot/certbot certonly --email <user@email.com> --logs-dir /etc/letsencrypt/logs
```

1を選択し、次に指示に従ってください。

```Bash
openssl dhparam -out ./bwdata/letsencrypt/live/<your.domain.com>/dhparam.pem 2048
./bitwarden.sh rebuild
./bitwarden.sh start
```

パワーシェル

> **Tip**
> Windows用のOpenSSLのビルドをインストールする必要があります。

```Bash
.\bitwarden.ps1 -stop
mv .\bwdata\letsencrypt .\bwdata\letsencrypt_backup
mkdir .\bwdata\letsencrypt
docker pull certbot/certbot
docker run -i --rm --name certbot -p 443:443 -p 80:80 -v <Full Path from \ >\bwdata\letsencrypt\:/e
tc/letsencrypt/ certbot/certbot certonly --email <user@email.com> --logs-dir /etc/letsencrypt/logs
Select 1, then follow instructions
<path/to/openssl.exe> dhparam -out .\bwdata\letsencrypt\live\<your.domain.com>\dhparam.pem 2048
.\bitwarden.ps1 -rebuild
.\bitwarden.ps1 -start
```

既存のSSL証明書を使用する

あなたは代わりに既存のSSL証明書を使用することも選択できますが、その場合は次のファイルが必要になります:

- サーバー証明書 (`certificate.crt`)
- プライベートキー (`private.key`)
- CA証明書 (`ca.crt`)

SSL信頼エラーを防ぐために、主要な証明書を中間CA証明書とバンドルする必要があるかもしれません。CA証明書を使用する際には、すべての証明書をサーバー証明書ファイルに含めるべきです。ファイルの最初の証明書はあなたのサーバー証明書であるべきで、その後に中間CA証明書が続き、最後にルートCAが続きます。

デフォルトの設定の下では、ファイルを `./bwdata/ssl/your.domain` に配置してください。
あなたの証明書ファイルの場所を変更するには、 `./bwdata/config.yml` の以下の値を編集してください :

```Bash
ssl_certificate_path: <path>
ssl_key_path: <path>
ssl_ca_path: <path>
```

Note

`config.yml`で定義された値は、NGINXコンテナ内の場所を表しています。ホスト上のディレクトリは、NGINXコンテナ内のディレクトリにマッピングされます。デフォルトの設定下では、マッピングは次のように一致します:

以下の値が`config.yml`にあります:

```
Bash

ssl_certificate_path: /etc/ssl/your.domain/certificate.crt
ssl_key_path: /etc/ssl/your.domain/private.key
ssl_ca_path: /etc/ssl/your.domain/ca.crt
```

次のホスト上のファイルへのマップ：

```
Bash

./bwdata/ssl/your.domain/certificate.crt
./bwdata/ssl/your.domain/private.key
./bwdata/ssl/your.domain/ca.crt
```

./bwdata/ssl/**内のファイルを操作するだけで済みます**。**NGINXコンテナーで直接ファイルを操作することはお勧めしません。**

Diffie-Hellmanキー交換を使用する

オプションとして、Diffie-Hellmanキー交換を使用して一時的なパラメータを生成する場合：

- 同じディレクトリに`dhparam.pem`ファイルを含めてください。
- `ssl_diffie_hellman_path:`の値を`config.yml`の設定に設定してください。

Note

あなたはOpenSSLを使用して自分自身の`dhparam.pem`ファイルを作成することができます。`openssl dhparam -out ./dhparam.pem 2048`を使用してください。

自己署名証明書を使用する

あなたは自己署名証明書を使用することも選択できますが、これはテストのみに推奨されます。

自己署名証明書は、デフォルトではBitwardenクライアントアプリケーションに信頼されません。この証明書を手動でインストールし、Bitwardenを使用する予定の各デバイスの信頼できるストアに追加する必要があります。

自己署名証明書を生成します。

```
Bash

mkdir ./bwdata/ssl/bitwarden.example.com
openssl req -x509 -newkey rsa:4096 -sha256 -nodes -days 365 \
  -keyout ./bwdata/ssl/bitwarden.example.com/private.key \
  -out ./bwdata/ssl/bitwarden.example.com/certificate.crt \
  -reqexts SAN -extensions SAN \
  -config <(cat /usr/lib/ssl/openssl.cnf <(printf '[SAN]\nsubjectAltName=DNS:bitwarden.example.com
\nbasicConstraints=CA:true')) \
  -subj "/C=US/ST=New York/L=New York/O=Company Name/OU=Bitwarden/CN=bitwarden.example.com"
```

あなたの自己署名証明書（`.crt`）と秘密鍵（`private.key`）は、`./bwdata/ssl/self/your.domain`ディレクトリに配置し、`./bwdata/config.yml`で設定することができます。

```
Bash

 ssl_certificate_path: /etc/ssl/bitwarden.example.com/certificate.crt
 ssl_key_path: /etc/ssl/bitwarden.example.com/private.key
```

自己署名証明書を信頼する

ウィンドウズ

Windowsで自己署名証明書を信頼するには、`certmgr.msc`を実行し、証明書を信頼されたルート認証機関にインポートしてください。

リナックス

Linuxで自己署名証明書を信頼するには、証明書を以下のディレクトリに追加してください:

```
Bash

/usr/local/share/ca-certificates/
/usr/share/ca-certificates/
```

次のコマンドを実行してください：

```Bash
sudo dpkg-reconfigure ca-certificates
sudo update-ca-certificates
```

私たちのLinuxデスクトップアプリ、Chromiumベースのブラウザを使用してウェブ保管庫にアクセスし、
ディレクトリコネクタデスクトップアプリの場合、このLinux証明書管理手順も完了する必要があります。

Bitwarden CLIとDirectory Connector CLIのために、自己署名証明書はローカルファイルに保存され、例えば`NODE_EXTRA_CA_CERTS=`環境変数によって参照されなければなりません。

```Bash
export NODE_EXTRA_CA_CERTS=~/.config/Bitwarden/certificate.crt
```

アンドロイド

Androidデバイスで自己署名証明書を信頼するには、Googleの証明書の追加と削除のドキュメンテーションを参照してください。

> **Note**
> あなたが**自己ホスト型ではない**場合、そしてあなたのアンドロイドデバイスで次の証明書エラーに遭遇した場合：
>
> ```Bash
> Exception message: java.security.cert.CertPathValidatorException: Trust anchor for certification path not found.
> ```
>
> あなたのデバイスにBitwardenの証明書をアップロードする必要があります。証明書の探し方については、
> このコミュニティスレッドを参照してください。

証明書を使用しないでください

> ⚠ **Warning**
>
> 証明書を使用しないことを選択した場合、
> **SSL経由でBitwardenを提供するプロキシでインストールをフロントにしなければなりません。**これは、
> BitwardenがHTTPSを必要とするためです。HTTPSプロトコルなしでBitwardenを使用しようとするとエラーが発生します。