bitwarden | Hilfezentrum Artikel

SELF-HOSTING

Zertifikatsoptionen

Ansicht im Hilfezentrum:
https://bitwarden.com/help/certificates/

Zertifikatsoptionen

Dieser Artikel definiert die Zertifikatsoptionen, die für selbst gehostete Instanzen von Bitwarden verfügbar sind. Sie wählen Ihre Zertifikatsoption während der Installation aus.

> **Note**
> Die Informationen in diesem Artikel sind möglicherweise nicht auf selbst gehostete Bitwarden Unified-Bereitstellungen anwendbar.

Generieren Sie ein Zertifikat mit Let's Encrypt

Let's Encrypt ist eine Zertifizierungsstelle (CA), die vertrauenswürdige SSL-Zertifikate kostenlos für jede Domain ausstellt. Das Bitwarden-Installationsskript bietet die Möglichkeit, ein vertrauenswürdiges SSL-Zertifikat für Ihre Domain mit Let's Encrypt und Certbot zu generieren.

Die Überprüfung der Zertifikatsverlängerung erfolgt jedes Mal, wenn Bitwarden neu gestartet wird. Die Verwendung von Let's Encrypt erfordert, dass Sie eine E-Mail-Adresse für Erinnerungen an das Ablaufdatum des Zertifikats eingeben.

Die Verwendung von Let's Encrypt erfordert, dass die Ports 80 und 443 auf Ihrem Gerät geöffnet sind.

Aktualisieren Sie ein Let's Encrypt Zertifikat manuell

Wenn Sie den Domainnamen Ihres Bitwarden-Servers ändern, müssen Sie Ihr generiertes Zertifikat manuell aktualisieren. Führen Sie die folgenden Befehle aus, um ein Backup zu erstellen, Ihr Zertifikat zu aktualisieren und Bitwarden neu aufzubauen:

Bash

```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
```

Wählen Sie 1, dann folgen Sie den Anweisungen:

```
Bash

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

PowerShell

> **Tip**
> Sie müssen eine Version von OpenSSL für Windows installieren.

```
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
```

Verwenden Sie ein vorhandenes SSL-Zertifikat

Sie können alternativ dazu wählen, ein bestehendes SSL-Zertifikat zu verwenden, was erfordert, dass Sie die folgenden Dateien haben:

- Ein Server-Zertifikat (`certificate.crt`)
- Ein privater Schlüssel (`private.key`)
- Ein CA-Zertifikat (`ca.crt`)

Sie müssen möglicherweise Ihr Hauptzertifikat mit Zwischen-CA-Zertifikaten bündeln, um SSL-Vertrauensfehler zu verhindern. Alle Zertifikate sollten in der Serverzertifikatdatei enthalten sein, wenn ein CA-Zertifikat verwendet wird. Das erste Zertifikat in der Datei sollte Ihr Serverzertifikat sein, gefolgt von jeglichen Zwischen-CA-Zertifikaten, gefolgt von dem Root-CA.

Unter der Standardkonfiguration platzieren Sie Ihre Dateien in `./bwdata/ssl/your.domain`. Sie können einen anderen Speicherort für Ihre Zertifikatsdateien festlegen, indem Sie die folgenden Werte in `./bwdata/config.yml` bearbeiten:

```
Bash

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

Note

Die in `config.yml` definierten Werte repräsentieren Standorte innerhalb des NGINX-Containers. Verzeichnisse auf dem Host werden Verzeichnissen innerhalb des NGINX-Containers zugeordnet. Unter der Standardkonfiguration richten sich die Zuordnungen wie folgt aus:

Die folgenden Werte in `config.yml`:

```
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
```

Karte zu den folgenden Dateien auf dem Host:

```
Bash

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

Sie sollten nur mit Dateien in `./bwdata/ssl/` arbeiten müssen. Es wird nicht empfohlen, direkt mit Dateien im NGINX-Container zu arbeiten.

Verwendung des Diffie-Hellman-Schlüsselaustauschs

Optional, wenn Diffie-Hellman Schlüsselaustausch verwendet wird, um ephemere Parameter zu generieren:

- Fügen Sie eine `dhparam.pem` Datei im selben Verzeichnis hinzu.
- Setzen Sie den Wert für `ssl_diffie_hellman_path:` in `config.yml`.

Note

Sie können Ihre eigene `dhparam.pem` Datei mit OpenSSL erstellen, indem Sie `openssl dhparam -out ./dhparam.pem 2048` verwenden.

Verwendung eines selbstsignierten Zertifikats

Sie können alternativ auch ein selbstsigniertes Zertifikat verwenden, dies wird jedoch nur für Tests empfohlen.

Selbstsignierte Zertifikate werden standardmäßig nicht von Bitwarden Client-Anwendungen vertraut. Sie müssen dieses Zertifikat manuell in den vertrauenswürdigen Speicher jedes Geräts installieren, das Sie mit Bitwarden verwenden möchten.

Generieren Sie ein selbstsigniertes Zertifikat:

```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"
```

Ihr selbstsigniertes Zertifikat (`.crt`) und privater Schlüssel (`private.key`) können im Verzeichnis `./bwdata/ssl/self/your.domain` platziert und in der `./bwdata/config.yml` konfiguriert werden:

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

Vertraue einem selbstsignierten Zertifikat

Fenster

Um einem selbstsignierten Zertifikat auf Windows zu vertrauen, führen Sie `certmgr.msc` aus und importieren Sie Ihr Zertifikat in die Vertrauenswürdigen Stammzertifizierungsstellen.

Linux

Um einem selbstsignierten Zertifikat unter Linux zu vertrauen, fügen Sie Ihr Zertifikat den folgenden Verzeichnissen hinzu:

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

Und führen Sie die folgenden Befehle aus:

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

Für unsere Linux-Desktop-App, den Zugriff auf den Web-Tresor mit Chromium-basierten Browsern und die Directory Connector Desktop-App, müssen Sie auch dieses Linux-Zertifikatsverwaltungsverfahren abschließen.

Für die Bitwarden CLI und Directory Connector CLI muss Ihr selbstsigniertes Zertifikat in einer lokalen Datei gespeichert und durch eine `NODE_EXTRA_CA_CERTS=` Umgebungsvariable referenziert werden, zum Beispiel:

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

Android

Um einem selbstsignierten Zertifikat auf einem Android-Gerät zu vertrauen, beziehen Sie sich auf die Dokumentation zum Hinzufügen & Entfernen von Zertifikaten von Google.

Note

Wenn Sie **nicht selbst hosten** und auf Ihrem Android-Gerät den folgenden Zertifikatsfehler feststellen:

```Bash
Exception message: java.security.cert.CertPathValidatorException: Trust anchor for certificati
on path not found.
```

Sie müssen die Zertifikate von Bitwarden auf Ihr Gerät hochladen. Beziehen Sie sich auf diesen Community-Thread, um Hilfe bei der Suche nach den Zertifikaten zu erhalten.

Verwenden Sie kein Zertifikat.

Warning

Wenn Sie sich dafür entscheiden, kein Zertifikat zu verwenden, **müssen Sie Ihre Installation mit einem Proxy versehen, der Bitwarden über SSL bereitstellt**. Dies liegt daran, dass Bitwarden HTTPS erfordert; der Versuch, Bitwarden ohne das HTTPS-Protokoll zu verwenden, wird Fehler auslösen.