Helix Coreに使用されるSSL証明書の更新手順を教えてください

質問

以下のメッセージが出力されHelix Coreサーバが起動しなくなりました。
SSL証明書はどのように更新すれば良いでしょうか？

メッセージ：
Perforce server error: Listen xxx.xxx.xxx.xxx:1666 failed Certificate date range invalid.

回答

以下の手順でSSL証明書を更新できます。

手順

> ⚠ **注意事項**
>
> ・"p4dctl"コマンドを使用してHelix Coreサーバを起動している場合、手順1から作業してください。
>
> ・"p4d"コマンドからHelix Coreサーバを起動している場合、手順1の"P4SSLDIR"の値をサーバ管理者に確認し、手順2から作業を進めてください。

1. "P4SSLDIR"の確認

以下のディレクトリに配置されている"master.conf"から"P4ROOT"と"P4SSLDIR"を確認します。

対象ディレクトリ：
/etc/perforce/p4dctl.conf.d

確認内容：
Environment { P4ROOT = /ssl_test/root P4USER = super P4SSLDIR = ssl

※"P4SSLDIR"が絶対パスで指定されていない場合、"P4ROOT"からの相対パスになります。
上記例の場合、"P4SSLDIR"は"/ssl_test/root/ssl"となります。

2. 既存証明書の退避

"/ssl_test/root/ssl"に配置されている[certificate.txt]と[privatekey.txt]を任意のディレクトリへ退避します。

ここでは、"/tmp"へ移動した例を紹介します。

コマンド例：
$ mv /ssl_test/root/ssl/certificate.txt /tmp $ mv /ssl_test/root/ssl/privatekey.txt /tmp

3. 環境変数"P4SSLDIR"の指定

OSの"perforce"ユーザにスイッチし、"export"コマンドから"P4SSLDIR"を指定します。

コマンド例：
$ su - perforce $ export P4SSLDIR=/ssl_test/root/ssl

4. 証明書の更新

"perforce"ユーザのまま、以下のコマンドを実行し、証明書を更新します。

コマンド例：
$ p4d -r /ssl_test/root -Gc

5. 証明書確認

"P4SSLDIR"配下に証明書が作成されたことを確認します。

コマンド例：
$ ls -l /ssl_test/root/ssl/certificate.txt $ ls -l /ssl_test/root/ssl/privatekey.txt

期待する結果：
-rw-------. 1 perforce perforce 1172 4月 16 20:53 /ssl_test/root/ssl/certificate.txt -rw-------. 1 perforce perforce 1708 4月 16 20:53 /ssl_test/root/ssl/privatekey.txt

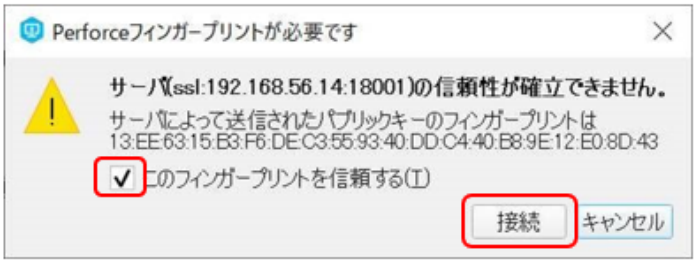
6. P4Dサーバの起動

証明書が作成されたことを確認した後、"p4dctl"コマンドからHelix Coreサーバを起動します。

7. フィンガープリントの更新　※クライアントとして操作します。

サーバ側の証明書が更新されたため、フィンガープリントの更新が必要です。

・P4Vからアクセスする場合
接続時に以下のダイアログが表示されます。
"このフィンガープリントを信用する"にチェックを入れ、[接続]をクリックします。



・コマンドラインの場合
"p4 trust"コマンドを実行します。
以下はサーバマシン上での更新例です。

既存のフィンガープリントがあるため、更新できなかった例

```
$ p4 -Ztag -p ssl:1666 trust

******* WARNING P4PORT IDENTIFICATION HAS CHANGED! *******
It is possible that someone is intercepting your connection
to the Perforce P4PORT '127.0.0.1:1666'
If this is not a scheduled key change, then you should contact
your Perforce administrator.
The fingerprint for the mismatched key sent to your client is
13:EE:63:15:B3:F6:DE:C3:55:93:40:DD:C4:40:B8:9E:12:E0:8D:43
Can't trust mismatched P4PORT key without the '-f' force option.
```

”-f”オプションを使用して強制的に更新する

```
$ p4 -p ssl:1666 trust -f

******* WARNING P4PORT IDENTIFICATION HAS CHANGED! *******
It is possible that someone is intercepting your connection
to the Perforce P4PORT '127.0.0.1:1666'
If this is not a scheduled key change, then you should contact
your Perforce administrator.
The fingerprint for the mismatched key sent to your client is
13:EE:63:15:B3:F6:DE:C3:55:93:40:DD:C4:40:B8:9E:12:E0:8D:43
Are you sure you want to establish trust (yes/no)? yes    ←入力する
Added trust for P4PORT 'ssl:1666' (127.0.0.1:1666)    ←yesと入力後に表示されるメッセージ
```

”p4 -Ztag info”コマンドから証明書の日付が更新されていることを確認します。

更新確認コマンド例

```
$ p4 -Ztag -p ssl:1666 info

...
... serverEncryption encrypted
... serverCertExpires Apr 16 11:53:15 2022 GMT
...
```