日日是Oracle APEX

Oracle APEXを使った作業をしていて、気の付いたところを忘れないようにメモをとります。

2022年11月22日火曜日

Oracle APEXの環境作成(10) - 自己署名証明書によるHTTPS化

自己署名証明書を生成し、ORDSへの接続をHTTPSに変更します。

自己署名証明書の生成

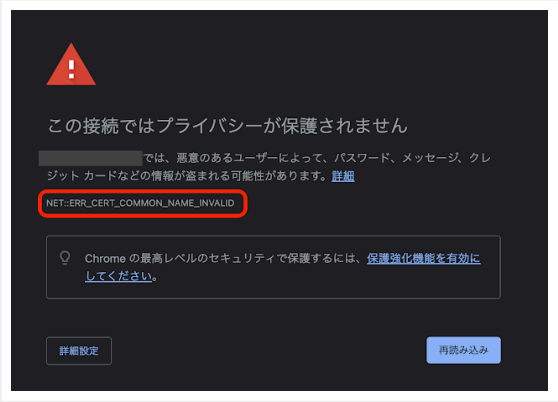
ORDSをインストールする際にプロトコルとしてHTTPSを選択すると、自己署名証明書を使用するか、または証明書と秘密鍵のファイルをそれぞれ指定するか、選択を要求されます。また、ホスト名の設定も要求されます。(以下はords installコマンドでの入力例です。これからの作業では設定ファイルを直接編集します。)

```
  Enter a number to select the protocol
    [1] HTTP
    [2] HTTPS
  Choose [1]: 2
  Enter the HTTPS port [8443]:
  Enter a number to select the certificate type
    [1] Use self-signed certificate (generates automatically)
    [2] Use my SSL certificate (requires SSL certificate and SSL certificate
private key)
  Choose [1]:
  Enter the SSL hostname: apex.mydomain.dev
  Enter the APEX static resources location: /home/oracle/i
```

自己署名証明書の使用を選択すると、ORDSが証明書と秘密鍵のファイルを作成し、それらのファイルを使ってORDSがHTTPSで接続の待ち受けを行うように構成されます。

ただし、Google ChromeやMicrosoft Edgeなどは証明書のSAN（Subject Alternative Name）としてホスト名が設定されていないと、接続時にエラーが発生します。ORDSが生成する自己署名証明書にはSANの設定が含まれていません。

自己署名証明書をPCに信頼できる証明書として登録してもエラーが発生します。以下はGoogle Chromeの例です。ブラウザによっては接続できますが、Google ChromeとMicrosoft Edgeでは不可です。



以下にSANを設定した自己署名証明書の作成手順を示します。ホスト名は**apex.mydomain.dev**としています。このホスト名については、それぞれ自分で割り与えるホスト名に変更してください。

手元のPCにホスト名からIPアドレスが解決できるように、/etc/hostsファイル（または同等のファイル）にエントリを追加しておきます。IPアドレスはコンピュート・インスタンスのパブリックIPを設定します。（VirtualBoxの仮想マシンでの作業であれば、127.0.0.1をIPアドレスとします）。

```
***.***.***.*** apex.mydomain.dev
```

sshで接続し、ユーザーrootに切り替えます。

最初にORDSを停止します。

systemctl stop ords

```
[root@localhost ~]# systemctl stop ords
[root@localhost ~]#
```

ORDSの実行ユーザーである、oracleに切り替えて作業を進めます。作業ディレクトリである/etc/ords/configへ移動します。

su - oracle
cd /etc/ords/config

```
[root@localhost ~]# su - oracle
Last login: Thu May 18 11:48:18 JST 2023 on pts/0
[oracle@localhost ~]$ cd /etc/ords/config
[oracle@localhost config]$
```

証明書と秘密鍵を配置するディレクトリglobal/standaloneを作成します。別の場所でも良いのですが、その場合は**settings.xml**のパラメータ**standalone.https.cert**、**standalone.https.cert.key**としてファイルを指定する必要があります。

ディレクトリ作成後、移動します。

mkdir global/standalone
cd global/standalone

```
[oracle@localhost config]$ mkdir global/standalone
[oracle@localhost config]$ cd global/standalone
[oracle@localhost standalone]$
```

OpenSSLを使って、自己署名証明書を生成します。

RSA公開鍵暗号のキーペアを鍵長2048ビットで生成します。ファイルは**private.pem**になります。

openssl genrsa -out private.pem 2048

CSR（Certificate Signing Request - 証明書署名要求）として**test.csr**を生成します。

国名などの入力を求められますが、共通名（Common Name）としてサーバー名が設定されていれば十分です。共通名以外はピリオドを入力することで、空白を設定しています。（何も入力しないと、デフォルトのXXなどが設定されます。）

openssl req -new -key private.pem -out test.csr

SAN（Subject Alternative Name）の設定に使用するファイル**san.txt**を作成します。

echo "subjectAltName = DNS:apex.mydomain.dev" > san.txt

自己署名証明書**self-signed.pem**を作成します。

openssl x509 -req -days 3650 -signkey private.pem -in test.csr -out self-signed.pem -extfile san.txt

秘密鍵のファイル**self-signed.key**を作成します。

openssl pkcs8 -topk8 -nocrypt -in private.pem -outform PEM -out self-signed.key

ORDSはsef-signed.pemおよびself-signed.keyを使用します。これらのファイル名はstandalone.https.cert、standalone.https.cert.keyのデフォルト値であるため、settings.xmlへの設定を省略できます。

```
[oracle@localhost standalone]$ openssl genrsa -out private.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
.....................................................+++++
e is 65537 (0x010001)
[oracle@localhost standalone]$ openssl req -new -key private.pem -out test.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:.
State or Province Name (full name) []:.
Locality Name (eg, city) [Default City]:.
Organization Name (eg, company) [Default Company Ltd]:.
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:apex.mydomain.dev
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

```
[oracle@localhost standalone]$ echo "subjectAltName = DNS:apex.mydomain.dev" >
san.txt
[oracle@localhost standalone]$ openssl x509 -req -days 3650 -signkey private.pem -
in test.csr -out self-signed.pem -extfile san.txt
Signature ok
subject=C = JP, L = Tokyo, O = Oracle, CN = apex.jp.oracle.com
Getting Private key
[oracle@localhost standalone]$ openssl pkcs8 -topk8 -nocrypt -in private.pem -
outform PEM -out self-signed.key
[oracle@localhost standalone]$
```

ORDSの設定変更

設定ファイル/etc/ords/config/settings.xmlを開きます。

```
[oracle@localhost ~]$ vi /etc/ords/config/global/settings.xml
[oracle@localhost ~]$
```

HTTPSを有効にする設定である**standalone.https.port**を追加します。**standalone.http.port**は削除します。HTTPSの待ち受けをするポート番号は8443とします。firewalldによりポート443への接続は8443へ転送されるように構成されているため、接続に使用するURLにポート番号を含む必要はありません。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Saved on Thu May 18 02:07:03 UTC 2023</comment>
<entry key="database.api.enabled">true</entry>
<entry key="standalone.context.path">/ords</entry>
<entry key="standalone.doc.root">/etc/ords/config/global/doc_root</entry>
<entry key="standalone.https.port">8443</entry>
<entry key="standalone.static.context.path">/i</entry>
<entry key="standalone.static.path">/home/oracle/i/</entry>
</properties>
```

ユーザーrootに戻ってORDSを起動します。

```
[root@localhost ~]# systemctl start ords
[root@localhost ~]#
```

サーバー側の設定は以上で完了です。

VirtualBoxでの作業の場合、仮想マシンのネットワーク設定にポート・フォワーディングを追加します。

ブラウザより、Oracle APEXの環境に接続すると証明書が不正と報告されます。

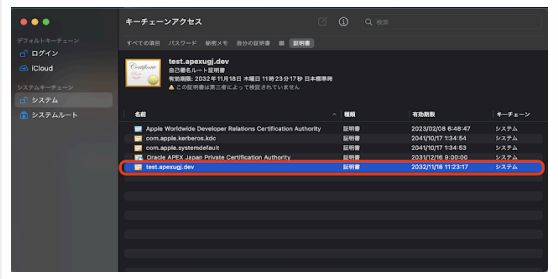
https://apex.mydomain.dev/ords/apex_admin
または（VirtualBoxの場合）
https://apex.mydomain.dev:8443/ords/apex_admin

NET::ERR_CERT_AUTHORITY_INVALIDをクリックするとPEM encoded chainとして自己署名証明書が表示されます。エラーを回避するには、この証明書を信頼させる必要があります。

信頼できる証明書の追加（macOSの例）

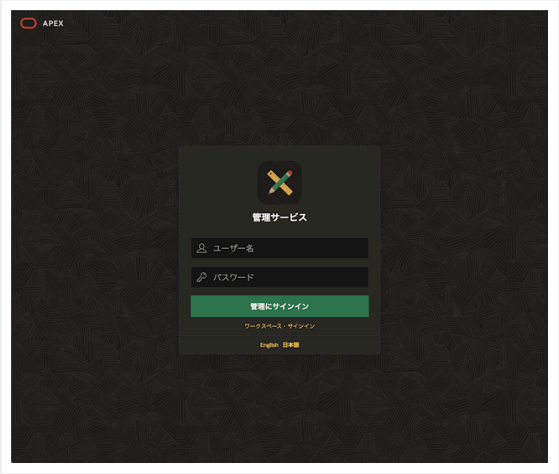
macOSの場合は、**キーチェーンアクセス**に証明書を登録します。

PEM encoded chainとして表示されている証明書をファイルにコピー＆ペーストし、キーチェーンアクセスにドロップします。



登録した証明書の情報を表示させ（ダブルクリックまたはコンテキスト・メニューの情報を見る）、**信頼**の**SSL(Secure Socket Layer)**を**常に信頼**に変更します。

以上の変更で、Oracle APEXにHTTPSで接続できるようになります。



続く

Yuji N. 時刻: 15:24

共有

‹ ホーム ›

ウェブ バージョンを表示

自己紹介

Yuji N.

日本オラクル株式会社に勤務していて、Oracle APEXのGroundbreaker Advocateを拝命しました。
こちらの記事につきましては、免責事項の参照をお願いいたします。

詳細プロフィールを表示