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28日月曜日

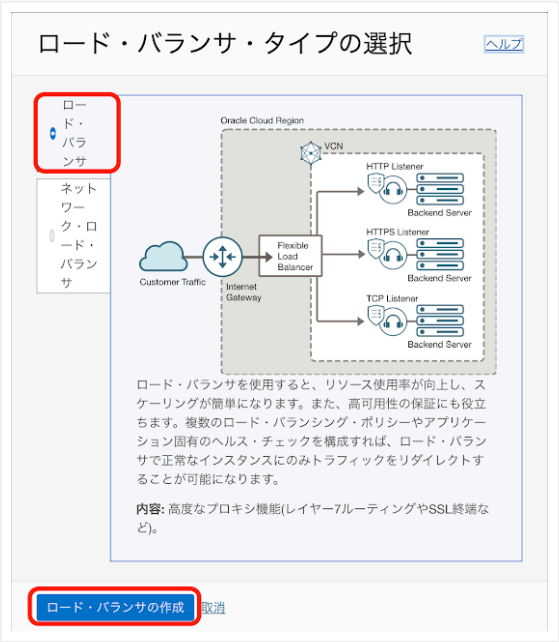
ロード・バランサを構成しORDSの可用性を確保する(2) - ロード・バランサの作成

Customer Managed ORDSが実行されている２つのコンピュート・インスタンスのフロントとなるロード・バランサを作成します。バックエンドはHTTP接続をポート8080で待ち受けます。ロード・バランサはHTTPS接続を標準のポート443で待ち受けます。サーバー証明書として、OCIの証明書サービスで作成したものを使用します。

ロード・バランサの作成

OCIのコンソールより**ネットワーキング**の**ロード・バランサ**を開きます。**ロード・バランサの作成**をクリックします。

ロード・バランサ・タイプの選択として、**ロード・バランサ**を選択します。**ロード・バランサの作成**をクリックします。



ロード・バランサ名は任意です。今回は**lb-testserv**としました。**可視性タイプの選択**は**パブリック**、**パブリックIPアドレスの割当て**は**エフェメラルIPアドレス**を選択します。Always Free枠のロード・バランサの**シェイプ**の**最小帯域幅**および**最大帯域幅**は、ともに**10Mbps**です。

ネットワーキングの選択に含まれる**仮想クラウド・ネットワーク**および**サブネット**として、あらかじめ作成済みのネットワークを指定します。

次へ進みます。

ロード・バランシング・ポリシーの指定として**重み付けラウンド・ロビン**を選択します。

バックエンドの追加をクリックしてバックエンドを追加します。

画面右にドロワーが開きます。ロード・バランサのバックエンドとなるコンピュート・インスタンス（今回の例では**CMRODS1**と**CMORDS2**）を選択します。

選択したバックエンドの追加をクリックし、ドロワーを閉じます。

バックエンド・サーバーが追加されます。このとき、**ポート**が80になっていたら**8080**へ変更します。ORDSは、ポート番号は8080でHTTP接続を待ち受けるように構成されています。

ヘルス・チェック・ポリシーの指定に含まれる**ポート**は**8080**、**ステータス・コード**は**302**、**URLパス(URI)**は**/ords**とします。バックエンドの通信はHTTPなので、**SSLの使用**に**チェックは入れません**。

次へ進みます。

リスナー名は任意です。今回は**lsnr-testserv**としました。**トラフィックのタイプ**は**HTTPS**、**モニターするポート**はデフォルトの**443**のままとします。

SSL証明書の**証明書リソース**として**証明書サービス管理対象証明書**を選択します。**証明書**として、先ほど作成した**TestServ**を選択します。

次へ進みます。

ロギングの管理は今回の検証の対象ではないため、**エラー・ログ**、**アクセス・ログ**ともに**OFF**にします。

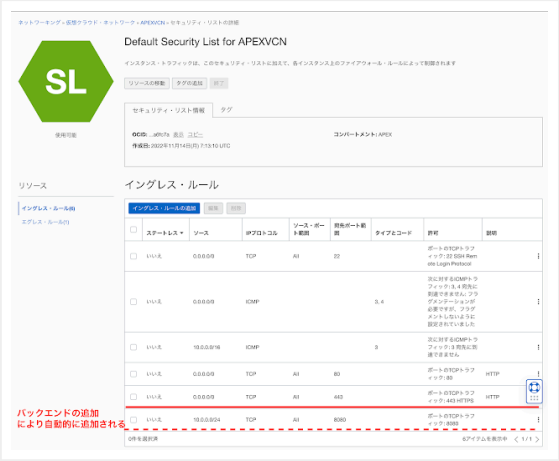
以上で**送信**をクリックします。

ロード・バランサが作成されます。ロード・バランサに割り当てられた**IPアドレス(パブリック)**を確認します。

以上でOracle APEXに接続可能になっています。

ロード・バランサへの接続を許可するため、ロード・バランサが配置されているネットワークにポート443への接続を許可するイングレス・ルールが設定済みであることを確認します。

ポート8080への接続を許可するイングレス・ルールは、ロード・バランサにバックエンドを追加したときに自動的に追加されます。



バックエンドの削除と追加を繰り返すと、同じイングレス・ルールが複数行になります。稼働に問題はありませんが、気になる場合は重複行を削除すると良いでしょう。

接続確認

作成した環境に接続します。/etc/hostsファイルまたはそれに準ずるファイルにパブリックIPアドレスとホスト名のペアを記述します。

IPアドレスはロード・バランサのパブリックIPアドレス、ホスト名は証明書の共通名またはSANとして設定したホスト名です。

```
129.***.***.218 testserv.******.dev
```

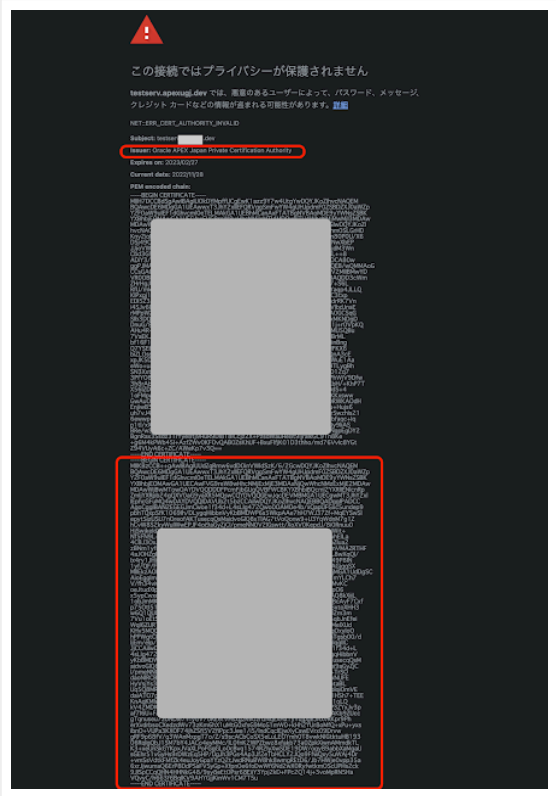
手元のPCに設定したホスト名にて、Oracle APEXの環境に接続します。

サーバー証明書の署名を行なっているCAは、プライベートCAであるため証明書に関するエラーが発生します。対応方法は、自己署名証明書を使用してHTTPS化したときと概ね同じです。

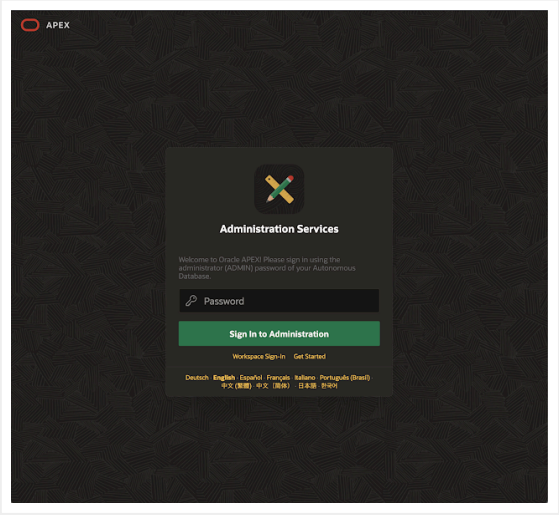
Oracle APEXの環境作成(10) - 自己署名証明書によるHTTPS化
http://apexugj.blogspot.com/2022/11/building-oracle-apex-environment-10-https.html

エラーが発生しているサーバー証明書を表示します。

自己署名証明のときと異なり複数の証明書が表示されます。一般に、後に表示されている証明書が上位の認証局の証明書になるため、その証明書をコピーしてPCに信頼できる証明書として登録します。



以上で、Oracle APEXの環境に接続できるようになります。



自己署名証明書の場合と異なり、一度、プライベートCAの証明書を登録すると、そのCAで署名されたサーバー証明書はすべて正しいサーバー証明書として扱われます。そのため、証明書をPCに登録する作業は、サーバーの数によらず一度で済みます。

完

Yuji N. 時刻: 16:40

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