

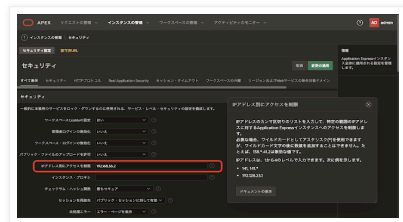
日々はOracle APEX

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。

2021年4月14日水曜日

IPアドレスによるアクセス制限が、どこのIPアドレスなのか確認する

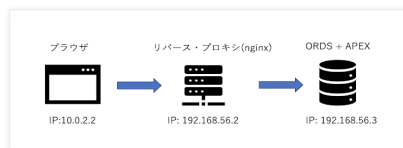
Oracle APEXの管理サービスのインスタンスの管理のセキュリティの設定に、IPアドレス別にアクセスを制限という設定があります。英語ではRestrict Access by IP Addressです。



管理系のサービスへのアクセスを、指定したIPアドレスに制限する設定です。IPアドレスはカンマ区切りで複数指定でき、またワイルド・カードとして(*)アスタリスクも指定できます

Autonomous Databaseでは、セキュリティの設定を行う画面は取り除かれています。しかし、プロシージャ [APEX_INSTANCE_ADMIN.SET_PARAMETER](#) を呼び出すことにより、この値を設定することができます。引数p_parameterに指定するパラメータは、[RESTRICT_IP_RANGE](#)です。

手元のMacのVirtualBoxを使って、ORDSとAPEXを入れた仮想マシンと、nginxを入れた仮想マシンを作成し、以下のように構成しました。ブラウザのIPかリバース・プロキシのIPか、どちらで制限されるのか確認してみました。



結論を先に記載します。リバース・プロキシのIPアドレスが考慮されます。より正確には、**APEXに一番近いIPアドレス**のようで、ブラウザが直結する場合は、ブラウザのIPアドレスが制限の対象になっています。

以下に確認のために行った作業を記載します。

最初にnginxをリバース・プロキシとして動かすために、以下の設定を追加しています。

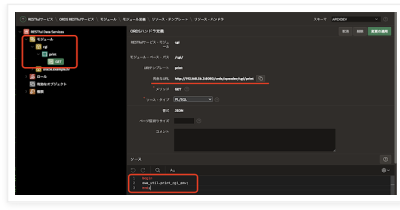
```
location /ords/ {
    proxy_pass http://192.168.56.3:8080/ords/;
    proxy_set_header Origin "";
    proxy_set_header X-Forwarded-Host $host:$server_port;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_connect_timeout 600;
    proxy_send_timeout 600;
    proxy_read_timeout 600;
    send_timeout 600;
}
```

ORDS、nginxともにプロトコルは暗号化はせずhttpで通信を行い、ポート番号として8080を指定しています。

APEXが受け取るHTTPヘッダーの情報を確認するため、RESTサービスを作成しました。

モジュールを作成しモジュール名をcgi、ベース・パスを/cgi/とします。そのモジュールにURLテンプレートとしてprintを作成します。作成したテンプレートにHTTPメソッドがGETのハンドラを作成します。ソース・タイプにPL/SQLを選択し、ソースとして以下を記載します。

```
begin
owa_util.print_cgi_env;
end;
```



作成したRESTサービスにアクセスする完全なURLは

http://192.168.56.3:8080/ords/apexdev/cgi/print

となっていますが、今回の構成では以下のURLでアクセスします。

http://localhost:8080/ords/apexdev/cgi/print

localhost(つまりVirtualBoxがインストールされているMac本体)の8080ポートを、nginxが動作している仮想マシンの8080ポートへポート・フォワーディングする設定を行っています。そのため、上記のURLでnginxのリバース・プロキシ経由でAPEX本体にアクセスされます。

アクセスした結果は以下になります。

```
REMOTE_IDENT =
REMOTE_USER = APEXDEV
Cookie = ORA_WWV_REMEMBER_LANG=ja
Accept = text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Forwarded-Host = localhost:8080
X-Forwarded-Proto = http
Connection = close
User-Agent = Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Sec-Fetch-Site = none
Sec-Fetch-Dest = document
Host = 192.168.56.3:8080
Accept-Encoding = gzip, deflate, br
Sec-Fetch-Mode = navigate
If-None-Match = "B1nTDOilpSeVcalQhB5gR/X2bS9CZkfOwd9IzrPlzBW5suPzLNNnpe8WBA3INBKTV70lt2sTEbDCI0qdvLVv8g=="
sec-ch-ua = "Google Chrome";v="89", "Chromium";v="89", ";Not A Brand";v="99"
sec-ch-ua-mobile = ?0
Upgrade-Insecure-Requests = 1
X-Forwarded-For = 10.0.2.2
Sec-Fetch-User = ?1
Accept-Language = ja,en-US;q=0.9,en;q=0.8
X-Real-IP = 10.0.2.2
APEX_LISTENER_VERSION = 20.4.1.r0131644
DAD_NAME =
DOC_ACCESS_PATH =
DOCUMENT_TABLE =
GATEWAY_IVERSION = 3
GATEWAY_INTERFACE = CGI/1.1
HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
HTTP_ACCEPT_ENCODING = gzip, deflate, br
HTTP_ACCEPT_LANGUAGE = ja,en-US;q=0.9,en;q=0.8
HTTP_ACCEPT_CHARSET =
HTTP_IF_MODIFIED_SINCE =
HTTP_IF_NONE_MATCH = "B1nTDOilpSeVcalQhB5gR/X2bS9CZkfOwd9IzrPlzBW5suPzLNNnpe8WBA3INBKTV70lt2sTEbDCI0qdvLVv8g=="
HTTP_HOST = 192.168.56.3:8080
HTTP_ORACLE_ECID =
HTTP_PORT = 8080
HTTP_REFERER =
HTTP_USER_AGENT = Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
PATH_ALIAS =
PATH_INFO = /print
PLSQL_GATEWAY = WebDb
QUERY_STRING =
REMOTE_ADDR = 192.168.56.2
REQUEST_CHARSET = AL32UTF8
REQUEST_IANA_CHARSET = UTF-8
REQUEST_METHOD = GET
REQUEST_PROTOCOL = http
REQUEST_SCHEME = http
SCRIPT_NAME = /ords/apexdev/cgi
SCRIPT_PREFIX =
SERVER_NAME = 192.168.56.3
SERVER_PORT = 8080
SERVER_PROTOCOL = HTTP/1.0
SERVER_SOFTWARE = Mod-Apex
WEB_AUTHENT_PREFIX =
X-APEX-METHOD = GET
X-APEX-BASE = http://192.168.56.3:8080/ords/apexdev/
X-APEX-PATH = cgi/print
X-APEX-REMOTE-ADDRESS = 192.168.56.2
X-APEX-CHARSET = UTF-8
HTTP_COOKIE = ORA_WWV_REMEMBER_LANG=ja
```

IPアドレスに関する情報は以下です。

```
X-Forwarded-For = 10.0.2.2
X-Real-IP = 10.0.2.2
REMOTE_ADDR = 192.168.56.2
```

X-Forwarded-For、X-Real-IPはnginxの設定で分かるように、nginxが設定しているものです。ですので、このサーバーが信頼できるかどうかが重要になります。REMOTE_ADDRはnginxが動作しているサーバーのIPアドレスです。

実際にIPアドレス制限を設定し、効果を確認します。アクセスできなくなると画面からIPアドレスの制限を設定できなくなるため、プロシージャを呼び出して設定します。

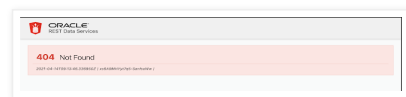
最初はRESTRICT_IP_RANGEに10.0.2.2を設定しています。

```
SQL> begin
  2  apex_instance_admin.set_parameter('RESTRICT_IP_RANGE','10.0.2.2');
  3  commit;
  4  end;
  5  /
```

PL/SQL procedure successfully completed.

SQL>

http://localhost:8080/ords/にアクセスすると404 Not Foundが発生します。



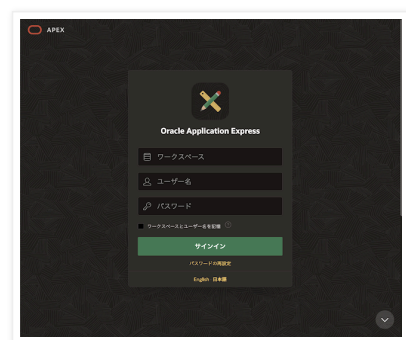
RESTRICT_IP_RANGEを192.168.56.2に変更します。

```
SQL> begin
  2  apex_instance_admin.set_parameter('RESTRICT_IP_RANGE','192.168.56.2');
  3  commit;
  4  end;
  5  /
```

PL/SQL procedure successfully completed.

SQL>

変更はcommitを実行した時点で反映されます。今度はサインイン画面が表示されます。



以上で確認作業は終了です。

Oracle APEXのアプリケーション作成の参考になれば幸いです。

追記

今回は中間にリバース・プロキシを入れましたが、すべてホスト名はlocalhost、ポート番号は8080でアクセスできるように構成しているため、とりあえずAPEXが使用できています。リバース・プロキシを使用するにはHTTPサーバーにも色々な設定が必要みたいです。

Peter Raganitschによる記事
[Tomcat with ORDS running APEX behind a reverse proxy](#)
[The Oracle APEX Reverse Proxy Guide using NGINX](#)
が参考になると思います。

Yuji N. 時刻: 18:45

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](#)

Powered by Blogger.