# 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。

2021年10月19日火曜日

## 要塞(Bastion)を使ってプライベート・ネットワーク上のコンピュート・インスタンスに接続する

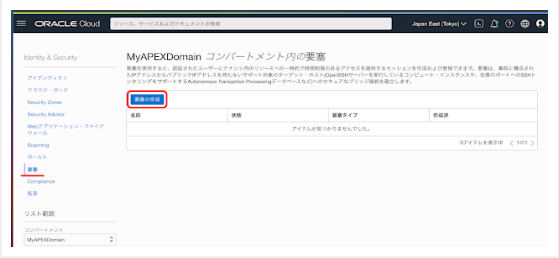
要塞(Bastion)を使って、プライベート・ネットワークにあるコンピュート・インスタンスに接続する方法を記述します。

以下の記述では、**コンパートメント名**が**MyAPEXDomain**、**仮想クラウド・ネットワーク**の名前もコンパートメント名と同じく**MyAPEXDomain**、その中に作成されている**プライベート・ネットワーク**の名前が**Private Subnet-MyAPEXDomain**であると仮定します。記事中のそれらの名称は、それぞれの環境に合わせて読み直す必要があります。接続先となる**コンピュート・インスタンス**の名前は**CMORDS1**としています。

コンパートメント名と仮想クラウド・ネットワークに同じ名前**MyAPEXDomain**が付けられています。そのため、説明が若干わかりにくくなってしまいました。

### 要塞(Bastion)を作成する

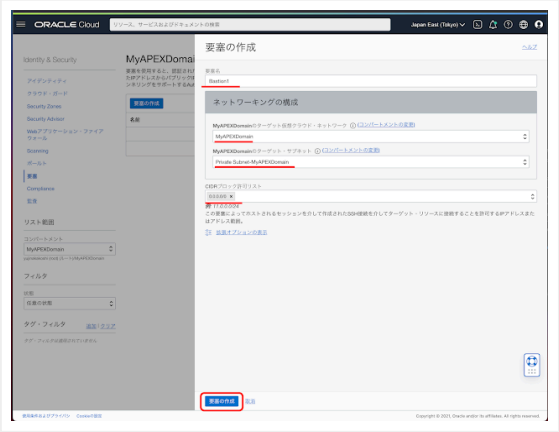
**Identity & Security**の**要塞**を開きます。**要塞の作成**をクリックします。



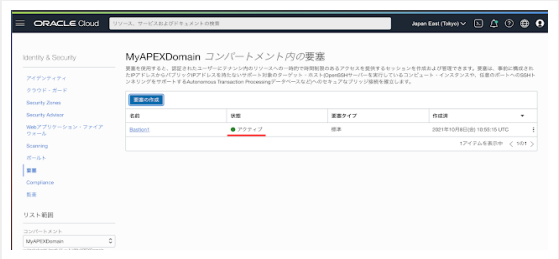

**要塞名**は**Bastion1**とします。**ネットワーキングの構成**の**MyAPEXDomainのターゲット仮想クラウド・ネットワーク**(このMyAPEXDomainはコンパートメント名)として**MyAPEXDomain**(このMyAPEXDomainはVCNの名前)、**MyAPEXDomainのターゲット・サブネット**として、接続するコンピュート・インスタンスが配置されているサブネットを選択します。ここでは**Private Subnet-MyAPEXDomain**を選択しています。**CIDRブロック許可リスト**には**0.0.0.0/0**を指定します。とりあえず、ネットワークのどこからでも要塞に接続できるようにしています。

**CIDRブロック許可リスト**として**0.0.0.0/0**を入力した後にEnterを入力すると0.0.0.0/0の入力が確定します。

**要塞の作成**をクリックします。



**Bastion1**の**状態**が**アクティブ**になると、要塞の完成です。

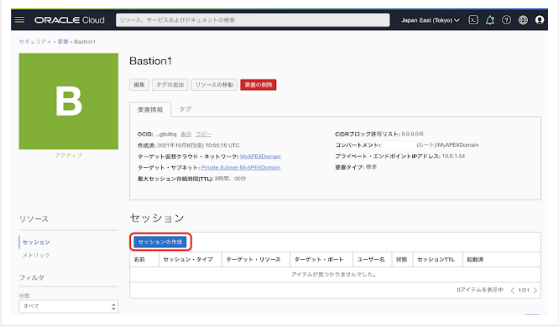


## コンピュート・インスタンスへファイルをアップロードする

**要塞(Bastion)**を通して、ファイルをコンピュート・インスタンスへアップロードします。そのために、要塞にて**SSHポート転送セッション**を作成します。

**Identity & Security**の**要塞**のページを開きます。作成済みの要塞**Bastion1**を開きます。

Bastion1にて、**セッションの作成**をクリックします。



ドロワーが開きます。**セッション・タイプ**として**SSHポート転送セッション**を選びます。**セッション名**は**Session-年月日-時刻**となるので、それはそのまま使います。作成したセッションの有効期間はデフォルトで３時間なので、セッション名から有効期間が分かります。**ターゲット・ホストに接続**する指定として**インスタンス名**を使うように選択し、接続先となる**コンピュート・インスタンス**を指定します。今回は**CMORDS1**を指定しています。SSHの**ポート**番号である**22**を転送先に選択します。

**SSHキーの追加**として**SSHキー・ファイルの選択**を選び、コンピュート・インスタンスCMORDS1を指定または生成した公開鍵ファイル(スクリーンショットでは**ssh-key-cmords1.key.pub**というファイルを指定しています)を**SSHキー**として指定します。

以上を設定して、**セッションの作成**をクリックします。


作成されたセッションが要塞の画面に一覧されます。


セッションの右端にある**ハンバーガー・メニュー**を開き、**SSHコマンドの表示**を実行します。


SSH接続を確立するためのSSHコマンドが表示されます。クリップ・ボードに**コピー**し、ダイアログを**閉じます**。


コピーしたsshコマンドは以下のような形式になります。

```
ssh -i <privateKey> -N -L <localPort>:10.0.1.82:22 -p 22
ocid1.bastionsession.oc1.ap-tokyo-
1.amaaaaaawzoefcia4dtbwg5kixkgv3ixgsupn2625puytgcsvk6dyrch27bq@host.bastion.ap-
tokyo-1.oci.oraclecloud.com
```

このコマンドに含まれる**<privateKey>**と**<localPort>**の部分を置き換えます。要塞のOCIDやホスト名は適切な値が入っているので変更はしません。秘密キーのファイルは、セッションの作成時に与えた証明書(公開鍵)と対になる秘密キーになります(ここでは**ssh-key-cmords1.key**としています)。ローカル・ポートとして**10022**を使うことにすると、上記のコマンドは次のようになります。

```
% ssh -i ssh-key-cmords1.key -N -L 10022:10.0.1.82:22 -p 22
ocid1.bastionsession.oc1.ap-tokyo-
1.amaaaaaawzoefcia4dtbwg5kixkgv3ixgsupn2625puytgcsvk6dyrch27bq@host.bastion.ap-
tokyo-1.oci.oraclecloud.com
```

上記コマンドは実行したままにしておきます。

別のターミナルよりファイルのアップロードを実行します。**sftp**コマンドでローカルのポートである**10022**に接続し、**put**コマンドを実行します。以下の実行例では**Wallet_APEXDEV.zip**および**apexugj.dev.zip**というファイルをアップロードしています。

```
% sftp -i ssh-key-cmords1.key -P 10022 opc@localhost
Connected to localhost.
sftp> put Wallet_APEXDEV.zip
Uploading Wallet_APEXDEV.zip to /home/opc/Wallet_APEXDEV.zip
Wallet_APEXDEV.zip                            100%   21KB   1.3MB/s   00:00
sftp> put apexugj.dev.zip
Uploading apexugj.dev.zip to /home/opc/apexugj.dev.zip
apexugj.dev.zip                               100% 6762   752.1KB/s   00:00
sftp> exit
%
```

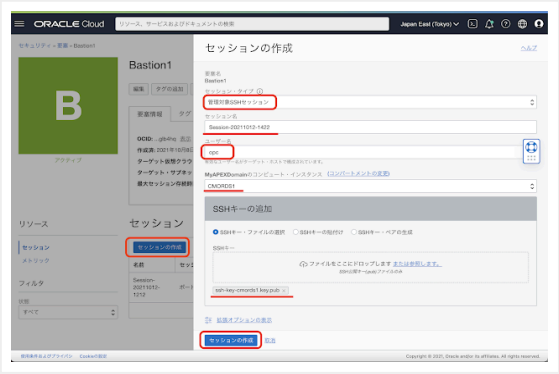
以上で、ファイルがユーザーopcのホーム・ディレクトリにアップロードされました。

これ以上アップロードするファイルがなければ、ポート転送を行なっているsshコマンドは終了できます。

## コンピュート・インスタンスへSSHで接続する

SSHでコンピュート・インスタンスに接続します。今度は要塞で**管理対象SSHセッション**を作成します。**要塞**の**Bastion1**を開き、**セッションの作成**を実行します。

**セッション・タイプ**として**管理対象SSHセッション**、**ユーザー名**に**opc**を指定する以外は、先ほどのポート転送セッションと同様の設定を行い、**セッションの作成**をクリックします。




セッションが作成されたら右端の**ハンバーガー・メニュー**を開き、**SSHコマンドのコピー**を実行します。


以下のようなsshコマンドがコピーされます。

```
ssh -i <privateKey> -o ProxyCommand="ssh -i <privateKey> -W %h:%p -p 22
ocid1.bastionsession.oc1.ap-tokyo-
1.amaaaaaawzoefciakq7z6smcwfodqn2ebveyeca7z7brmbn2dfgdmpox4dyq@host.bastion.ap-
tokyo-1.oci.oraclecloud.com" -p 22 opc@10.0.1.82
```

**<privateKey>**の部分を秘密キーのファイル名に置き換え、sshコマンドを実行します。

```
% ssh -i ssh-key-cmords1.key -o ProxyCommand="ssh -i ssh-key-cmords1.key -W %h:%p -
p 22 ocid1.bastionsession.oc1.ap-tokyo-
1.amaaaaaawzoefciakq7z6smcwfodqn2ebveyeca7z7brmbn2dfgdmpox4dyq@host.bastion.ap-
tokyo-1.oci.oraclecloud.com" -p 22 opc@10.0.1.82
The authenticity of host '10.0.1.82 (<no hostip for proxy command>)' can't be
established.
ECDSA key fingerprint is SHA256:oTItIYbGj7E26UZlk2dcXFqcBeZ5GXGUVbJXyn+IkJY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.82' (ECDSA) to the list of known hosts.
Activate the web console with: systemctl enable --now cockpit.socket

[opc@cmords1 ~]$
```

初回接続時はfingerprintをknown_hostsファイルに追加するかどうか確認を求められます。**yes**を入力すると宛先のコンピュート・インスタンスに接続されます。

以上で要塞を使って使ってプライベート・ネットワーク上のコンピュート・インスタンスに接続する方法の記事は終了です。

Oracle APEXをOracle Cloud上で構成する際の参考になれば幸いです。

**完**

Yuji N. 時刻: 13:44

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