ORACLE
Cloud Infrastructure

NATインスタンスの構成:

プライベート・サブネットのインターネット・アクセスの有効化

ORACLE WHITE PAPER | 2018年1月

ORACLE

目次

概要

Oracle Cloud Infrastructureを使用すると、クラウドにおける拡張データ・センターとして機能する仮想クラウド・ネットワーク(VCN)を作成できます。プラットフォームには仮想ネットワーキング・プリミティブが用意されており、複雑なエンタープライズ要件に対応するネットワークを構築する際の柔軟性が非常に高まります。VCNには任意のアドレス範囲を使用でき、それをサブネットにセグメント化して、セキュリティ・リストとルート表を構成できます。インターネットを使用するIPsec接続、または専用のプライベート接続を使用するFastConnectを介し、動的ルーティング・ゲートウェイ(DRG)を通してVCNをオンプレミス・ネットワークに接続できます。

ネットワーク設計の最も一般的な要件の1つは、プライベート・インスタンスを保護してインターネットからアクセスできないようにするだけでなく、オンプレミス・ネットワークまたはパブリック・サブネットの要塞ホストからのみアクセスできるようにすることです。この要件は、インスタンスをプライベート・サブネットで起動するか、起動時のパブリックIPアドレスの割当てを行わないことで実現できます。ただし、これらのバックエンド・インスタンスは、ソフトウェアの更新やCRL検証など、特定の目的でインターネットへのアクセスが必要になる場合があります。このトラフィックをインターネット・ゲートウェイを介してオンプレミス・ネットワークにルーティングすることもできますが、不要なレイテンシやコストが加わる可能性があります。

1993年、ネットワーク・アドレス変換(NAT)に関する最初の文書が公開されました。NATは、IPアドレスの枯渇を防ぐためにアドレス空間を再利用する方法だと考えられていましたが、プライベート・ネットワークをパブリック・インターネットに接続する方法として広く採用されました。

現在NATは、1つの外部アドレスの背後にIP領域全体を隠すことができる、IPマスカレードの形式として最も一般的に使用されています。認可されていないトラフィックはプライベート・ネットワークに入れないため、NATは事実上、付加的なファイアウォールとなっています。

Oracle Cloud Infrastructureの仮想ネットワーキング・プラットフォームが最近拡張され、NATインスタンスを使用して、プライベート・インスタンスからのアウトバウンドのインターネット・アクセスを有効化できるようになりました。このホワイト・ペーパーでは、VCNにNATインスタンスを設定する際と、インターネット・リクエストをルーティングできるようプライベート・サブネットを構成する際の推奨ステップを説明します。

前提

このホワイト・ペーパーは、プライベート・ネットワークのNATゲートウェイとして機能するインスタンスの構成を行うユーザーを対象としています。

このホワイト・ペーパーに説明されているとおりにデプロイメントを実行するには、次の事項に精通している必要があります。

- Linuxコマンド・ライン
- 広く普及している軽量で無料のデプロイメント・ツールであるTerraformを使用したクラウド・インフラストラクチャのプロビジョニング(https://www.terraform.io/intro/index.html)
- ネットワーキング・プロトコルに関する基礎知識

Oracle Cloud Infrastructureの基礎についても熟知している必要があります。詳細は、https://docs.us-phoenix-1.oraclecloud.com/を参照してください。プラットフォームを使用するのは今回が初めての場合は、特に、https://docs.us-phoenix-1.oraclecloud.com/Content/GSG/Reference/overviewworkflow.htmのチュートリアルをお薦めします。

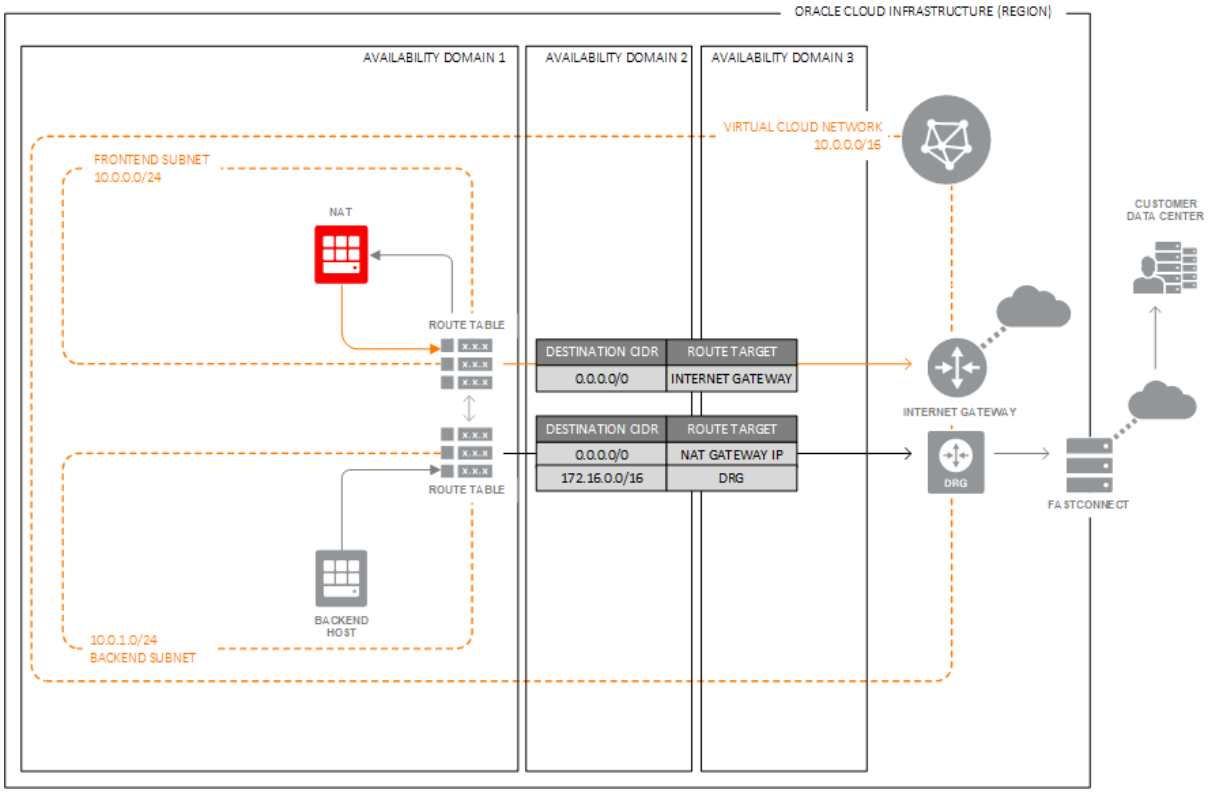
基本的なNATの構成

Oracle Cloud Infrastructure Networkingの特性により、仮想インタフェースを使用してサブネットを物理的に分離する必要はありません。ルーティングは基礎となるソフトウェアが定義したネットワーキングによって行われ、ほとんどの場合、サブネット間にセキュリティ・リストが存在するため、使用する仮想NIC (VNIC)は1つで十分です。そのため、このホワイト・ペーパーの例の大部分では、単一のインタフェースを使用しています。

複数のVNICを使用している場合は、ルーティング表が、接続しているサブネットのゲートウェイIPアドレスを正確に指していることを確認するか、Linuxカーネルのリバース・パス・フィルタリングを無効にしてください。

アーキテクチャ

次の図は、推奨する設定の大まかなアーキテクチャを示しています。



この図には、サブネットが2つあるVCN (NAT-VCN-1)が示されています。

- **パブリック**(10.0.0.0/24): インターネット・ゲートウェイを介してインターネットにアクセス可能です。**NAT1**は、フロントエンド・サブネットのインスタンスで、プライベート・サブネットのNATとして機能します。
- **プライベート**(10.0.1.0/24): インターネットにアクセスできないプライベート・サブネットです。**バックエンド・ホスト**は、プライベート・サブネットのインスタンスを表しています。

注意: プライベート・サブネットのポリシーにより、VNICからのパブリックIPアドレスの割当てが禁止されており、それが、外部アクセスに対する付加的なセキュリティ・レイヤーとなっています。

パブリック・サブネットの構成

パブリック・サブネットのルート表には、インターネット・ゲートウェイをすべてのトラフィックのルート・ターゲット(0.0.0.0/0)として構成するルート・ルールがあります。

セキュリティ・リストのエグレス・ルールでは、すべての宛先に対するトラフィックが許可されています。イングレス・ルールでは、バックエンド・サブネット(およびVCNのその他すべてのアドレス範囲)からのトラフィックが許可されています。

プライベート・サブネットの構成

プライベート・サブネットのルート表には、**NAT1**ホストをすべてのトラフィックのルート・ターゲット(0.0.0.0/0)として構成するルート・ルールがあります。

セキュリティ・リストのエグレス・ルールでは、すべての宛先に対するトラフィックが許可されています。イングレス・ルールでは、特定のアドレス範囲(オンプレミス・ネットワークやVCN内のその他すべてのバックエンド・サブネットなど)のみが許可されています。

オンプレミス・ネットワークとの接続を使用する場合は、エンタープライズに向かうルートを、構成済の**DRG**に設定する必要があります。

この構成では、バックエンド・インスタンスでアウトバウンドのインターネット・リクエストが開始されると、トラフィックが**NAT1**インスタンスにルーティングされます。**NAT1**インスタンスは、(ソースNATの適用後に)インターネット・ゲートウェイを介して、トラフィックをインターネットに転送します。インターネット上の宛先では、トラフィックのソースが、**NAT1**のパブリックIPアドレスであるとみなされます。NATインスタンスは、インターネットからレスポンスを受信すると、(宛先NATの適用後に)そのトラフィックをバックエンド・インスタンスに転送します。

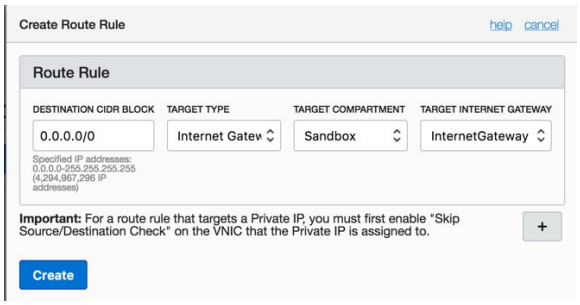
構成

この項では、ネットワークとNATインスタンスを作成する基本ステップの例を示します。

1. Oracle Cloud Infrastructureコンソールで、リソースのないVCNを作成します。そのVCNには、デフォルトの空のルート表と、デフォルトのセキュリティ・リスト、DHCPオプションが作成されます。この例では、そのVCNをNAT-VCN-1と呼びます。
2. 作成したVCNを開きます。「リソース」パネルで、「**セキュリティ・リスト**」をクリックして、デフォルトのセキュリティ・リストを開きます。「**すべてのルールの編集**」をクリックします。
3. イングレス・ルールを作成します。「**ソースCIDR**」フィールドに、「**10.0.1.0/24**」(お客様のプライベート・サブネット領域)と入力し、「**すべてのプロトコル**」を選択します。SSHプロトコルを許可するルールも作成できます。

4. 「**すべてのプロトコル**」に「**0.0.0.0/0**」を許可するエグレス・ルールを作成します。
5. 「**セキュリティ・リスト・ルールの保存**」をクリックします。

6. 「リソース」パネルで、「**インターネット・ゲートウェイ**」をクリックし、「**インターネット・ゲートウェイの作成**」をクリックします。
7. **InternetGateway**という名前を割り当て、「**インターネット・ゲートウェイの作成**」をクリックします。
8. 「リソース」パネルで、「**ルート表**」をクリックし、デフォルトのルート表を開きます。
9. 次の値を使用してデフォルトのルート表にルールを作成し、「**作成**」をクリックします。
    - **宛先:** 0.0.0.0/0
    - **ターゲット・タイプ:** インターネット・ゲートウェイ・ターゲット
    - **コンパートメント:** コンパートメントを選択します。
    - **ターゲットの選択:** InternetGateway



10. 「リソース」パネルで、「**サブネット**」をクリックし、「**サブネットの作成**」をクリックします。
11. 次の値を入力して、「**作成**」をクリックします。
    - **名前:** Public Subnet
    - **可用性ドメイン:** リストから選択します。
    - **CIDRブロック:** 10.0.0.0/24
    - **ルート表:** デフォルトのルート表NAT-VCN-1
    - **サブネット・アクセス:** パブリック・サブネット
    - **DHCPオプション:** NAT-VCN-1のデフォルトのDHCPオプション
    - **セキュリティ・リスト:** NAT-VCN-1のデフォルトのセキュリティ

    プライベート・サブネットを作成する前に、NATインスタンスを作成します。先にNATインスタンスを作成すると、NATインスタンスに割り当てられているプライベートIPのOCID(識別子)を、サブネットのルート表のルート・ターゲットとして選択できます。

12. 「**コンピュート**」メニューで、「**インスタンス**」をクリックし、「**インスタンスの起動**」をクリックします。インスタンスを次のように構成します。

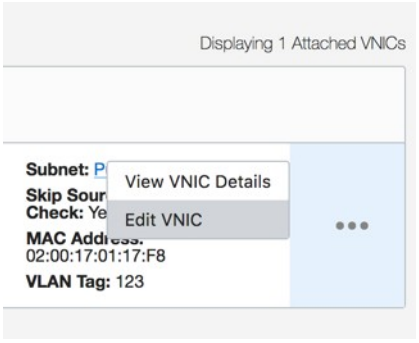
    - **名前:** NAT1
    - **可用性ドメイン:** サブネットを作成した可用性ドメインを選択します。
    - **イメージ:** Oracle-Linux-7.4-2017.08.24-1以降
    - **シェイプ:** VM.Standard1.2
    - **仮想クラウド・ネットワーク:** NAT-VCN-1
    - **サブネット:** Public Subnet
    - **プライベートIPアドレス:** 10.0.0.2
    - **パブリックIPアドレスの割当て:** このチェック・ボックスを選択します。
    - **SSHキー:** SSH鍵をアップロードするか貼り付けます。
    - 「**拡張オプションの表示**」をクリックして、「**Cloud-initスクリプトの貼付け**」オプションを選択し、次のテキストを貼り付けます。または、https://github.com/oracle/terraform-provider- oci/blob/master/docs/examples/networking/nat/user_data.tplからファイルをダウンロードし、アップロード機能を使用することも可能です。

      これにより、NATと、ネットワーク上のその他のホストにルーティング・サービスを提供するサーバー・ファイアウォールとカーネルが構成されます。

```
#cloud-config
write_files:
# Create file to be used when enabling ip forwarding
  - path: /etc/sysctl.d/98-ip-forward.conf
    content: |
      net.ipv4.ip_forward = 1
runcmd:
  # Run firewall commands to enable masquerading and port forwarding
  # Enable ip forwarding by setting sysctl kernel parameter
  - firewall-offline-cmd --direct --add-rule ipv4 nat POSTROUTING 0 -o ens3 -j MASQUERADE
  - firewall-offline-cmd --direct --add-rule ipv4 filter FORWARD 0 -i ens3 -j ACCEPT
  - /bin/systemctl restart firewalld
  - sysctl -p /etc/sysctl.d/98-ip-forward.conf
```

13. 「**インスタンスの作成**」をクリックします。

14. インスタンスの名前をクリックし、「**アタッチされたVNIC**」をクリックします。次に、「**VNICの編集**」をクリックします。



15. 「**ソース/宛先チェックのスキップ**」を選択してから、「**VNICの更新**」をクリックします。

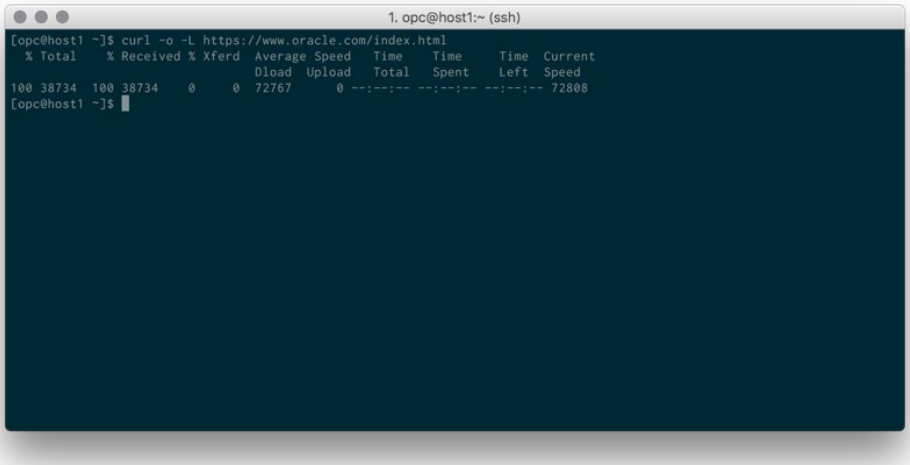
注意: このステップは重要です。実行しない場合、デフォルトで有効化されているセキュリティ機能が原因で、その他のインスタンスはNATゲートウェイを介してトラフィックを送信できません。ソース/宛先チェックがある状態でVNICにルート・ターゲットの構成を試行すると、エラー・メッセージが表示されます。

この時点で、必要なすべてのリソースがパブリック・サブネットに作成されています。次以降のステップでは、プライベート・ネットワークの作成プロセスを順を追って説明します。

16. **「ネットワーキング」>「仮想クラウド・ネットワーク」>「NAT-VCN-1」**に戻ります。
17. 「リソース」パネルで、「**セキュリティ・リスト**」をクリックして、「**セキュリティ・リストの作成**」をクリックします。
18. 次の値を入力して、「**セキュリティ・リストの作成**」をクリックします。
    - 名前に、「**Security List for Private Subnet**」と入力します。
    - 宛先が**0.0.0.0/0**で、「**すべてのプロトコル**」が選択されたエグレス・ルールを追加します。
    - お客様のニーズとセキュリティ・ポリシーに従って、イングレス・ルールを構成します。SSHトラフィックを許可するルールを、少なくとも1つ必ず追加してください。
19. 「リソース」パネルで、「**ルート表**」をクリックし、「**ルート表の作成**」をクリックします。
20. 次の値を入力して「**ルート表の作成**」をクリックします。
    - **名前:** Private Route
    - **宛先:** 0.0.0.0/0
    - **ターゲット・タイプ:** プライベートIP
    - **ターゲットの選択:** 10.0.0.2
21. 「リソース」パネルで、「**サブネット**」をクリックし、「**サブネットの作成**」をクリックします。

22. 次の値を入力して「**作成**」をクリックします。
    - **名前:** Private Subnet
    - **可用性ドメイン:** 可用性ドメインを選択します。
    - **CIDRブロック:** 10.0.1.0/24
    - **ルート表:** Private Route
    - **サブネット・アクセス:** プライベート・サブネット
    - **DHCPオプション:** NAT-VCN-1のデフォルトのDHCPオプション
    - **セキュリティ・リスト:** Security List for Private Subnet

これで、プライベート・サブネットの任意のオペレーティング・システムを使用して、ホスト・インスタンスを起動できます。パブリックIPアドレスが割り当てられていなくてもインターネットへの接続は可能で、インターネットが発生源の接続は、直接お客様のサーバーにアクセスすることはできません。プライベート・ホストを管理するには、SSHを使用して、まずNATインスタンスに接続するか、お客様独自のネットワークからCPE VPN接続を使用します。



Terraform

Terraformは、インフラストラクチャの構築、変更およびバージョニングを行うツールです。必要な状態に到達するために何を行うかを説明する実行計画を構成ファイルから生成し、インフラストラクチャを構築するための変更を実行します。Terraformの基本的な情報は、次のサイトを参照してください。

- https://github.com/oracle/terraform-provider-oci
- https://community.oracle.com/community/oracle-cloud/cloud-infrastructure/blog/2017/02/15/terraform-and-oracle-bare-metal-cloud-services

NATのサンプル構成は、https://github.com/oracle/terraform-provider-oci/tree/master/docs/examples/networking/natにある**terraform-provider-oci** Gitリポジトリの「**examples**」フォルダにあります。

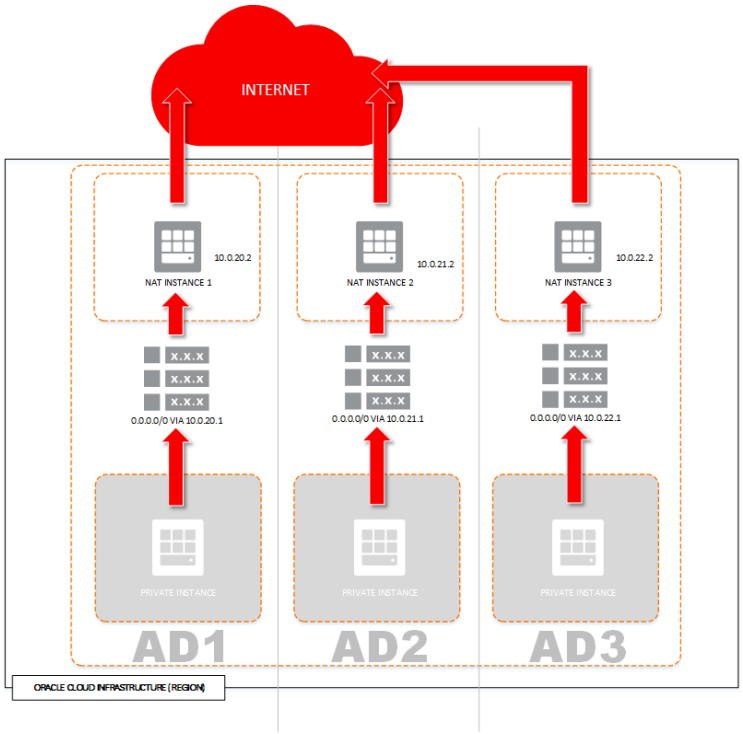
NAT HAおよび高度な概念

デプロイメントで複数の可用性ドメインを使用する場合は、なんらかの形でハートビートやフェイルオーバーのメカニズムを保有する必要があります。クラウド以外の一般的なデプロイメントでは、レイヤー2パスとIPフェイルオーバーを使用することでこれを実現できます。Oracle Cloud Infrastructure Networkingの特性上、冗長性を実現する最善の方法は、ルート表の構成を直接管理することです。

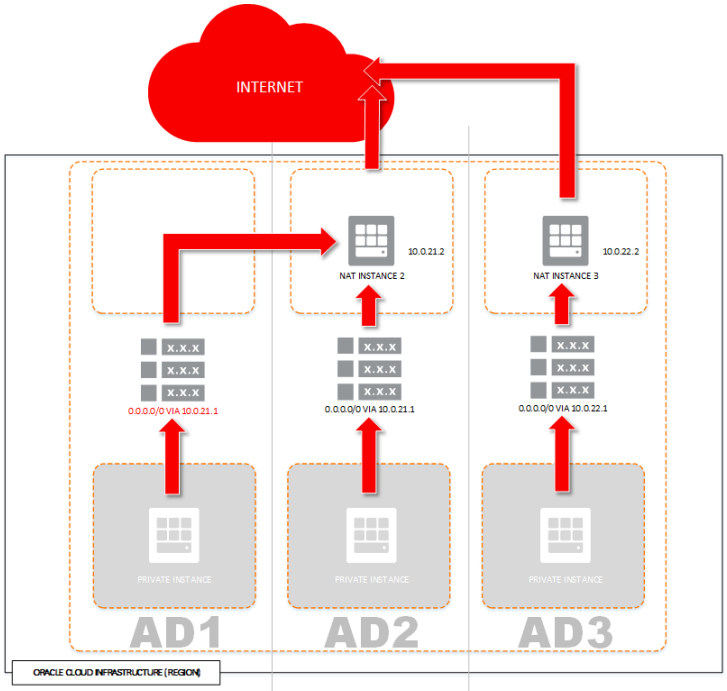
HAアーキテクチャ

次の図は、プライベート・サブネットにNATインスタンスとホストが存在する3つの可用性ドメインを示しています。

通常の状態であれば、トラフィックは可用性ドメイン内にとどまり、パブリック・サブネットのNATゲートウェイ上で変換されます。



NATゲートウェイに障害が発生した場合は、次の図に示すように、別の可用性ドメインのNATゲートウェイにトラフィックがフェイルオーバーします。



NATインスタンス1を使用できないため、NATインスタンス2が、AD1にあるプライベート・サブネットのルート表を引き継いで変更します。デフォルト・ゲートウェイは、プライベートIPの一意の識別子(OCID)を使用して、NATインスタンス2のプライベートIPをルート・ターゲットとして構成します。これにより、インスタンスに障害が発生した場合でも、プライベート・インスタンスがインターネットに到達できることが保証されます。

必要なリソースと作成順序

次の表に、前述のステップに必要なリソースをまとめてあります。デプロイメント・チェックリストとして使用できます。

VCN	依存性		
インターネット・ゲートウェイ	VCNに依存		
パブリック・ルート表AD1	VCNに依存		
パブリック・ルート表AD2	VCNに依存		
パブリック・ルート表AD3	VCNに依存		
プライベート・ルート表AD1	VCNに依存		
プライベート・ルート表AD2	VCNに依存		

VCN	依存性		
プライベート・ルート表AD3	VCNに依存		
パブリック・セキュリティ・リスト	VCNに依存		
プライベート・セキュリティ・リスト	VCNに依存		
パブリック・サブネットAD1	VCNに依存	ルート表に依存	セキュリティ・リストに依存
パブリック・サブネットAD2	VCNに依存	ルート表に依存	セキュリティ・リストに依存
パブリック・サブネットAD3	VCNに依存	ルート表に依存	セキュリティ・リストに依存
プライベート・サブネットAD1	VCNに依存	ルート表に依存	セキュリティ・リストに依存
プライベート・サブネットAD2	VCNに依存	ルート表に依存	セキュリティ・リストに依存
プライベート・サブネットAD3	VCNに依存	ルート表に依存	セキュリティ・リストに依存
NATインスタンスAD1	サブネットに依存		
NATインスタンスAD2	サブネットに依存		
NATインスタンスAD3	サブネットに依存		
プライベート・インスタンスAD1	サブネットに依存		
プライベート・インスタンスAD2	サブネットに依存		
プライベート・インスタンスAD3	サブネットに依存		
パブリック・サブネットのルート・ルール	インターネット・ゲートウェイに依存		
プライベート・サブネットのルート・ルール	NATインスタンス		

ルート・ルールの作成では、ターゲット・ルールへのルートに、NATインスタンスVNICにアタッチされている既存のプライベートIPオブジェクトが必要なため、NATインスタンスを先に起動する必要があることに注意してください。

HA構成

この例のHAでは、キープアライブ・デーモンと、フェイルオーバーを実行するカスタム・スクリプトが使用されています。また、コンパートメント内のvirtual-network-familyを管理するため、NATインスタンスには、Oracle Cloud Infrastructure CLI、API鍵、ユーザーIDおよび関連するポリシーが必要です。例:

```
Allow group NAT to manage virtual-network-family in compartment id
aaa.compartment.ocid
```

フェイルオーバー・スクリプト

フェイルオーバー・スクリプトは、メタデータ情報を処理し、指定されたルート表でルート・ルールの変更を行います。VRRPグループ内のアクティブなノードは、ルート・ルールがプライベートIPのOCIDを指すようにします。

スクリプトの例は、付録1を参照してください。

Keepalived.conf

VRRP構成では、3つの別々のインスタンスにキープアライブを構成する必要があります。それぞれのNATインスタンスがその可用性ドメインのマスター・ノードとなり、残りの2つがバックアップ状態になります。各VRRPインスタンスの`virtual_router_id`パラメータが違っていることと、マスター・ノードの優先度が高くなっていることを確認してください。

構成の例は、付録2を参照してください。

各ノードで、適切な可用性ドメイン内での優先度と、初期状態、ノードのIPアドレスを必ず更新してください。

結論

NATインスタンスは、クラウド・データ・センターの重要なリソースの保護や、プライベート・サブネットにあるホストへのサービスの提供に使用できます。プライベート・サブネットに配置されているサーバーは、VCNの外からのアクセスに対して保護されていますが、インターネットにはアクセスできます。

付録

付録1: notify.shの例

```
#!/bin/bash

STATUS=$1
AD=$2
RT_TABLE_ID=$3

CURL="/usr/bin/curl -s"
OCI=$(/usr/bin/oci)
MDS="http://169.254.169.254/opc/v1"
INSTANCE_MDS=$MDS"/instance"
VNIC_MDS=$MDS"/vnics"

PATH="/usr/libexec/keepalived"

PUB_SN_ID=$($CURL "$INSTANCE_MDS/metadata/subnet_id")
PRIV_SN_ID=$($CURL "$INSTANCE_MDS/metadata/private_subnet_id")
VNIC_ID=$($CURL "$VNIC_MDS/0/vnicId")
echo $VNIC_MDS
echo $VNIC_ID

echo $STATUS > $PATH/$AD"_status.txt"

$OCI network private-ip list --subnet-id $PUB_SN_ID --vnic-id $VNIC_ID |
/usr/bin/python -c 'import sys, json; print
json.load(sys.stdin)["data"][0]["id"]' > $PATH"/private_ip.ocid"



case "$STATUS" in
  "master") echo "master"
    if [ ! -z $RT_TABLE_ID ]; then
      PRIVATE_IP_ID=$(/bin/cat $PATH"/private_ip.ocid")
$OCI network route-table update --force --rt-id $RT_TABLE_ID --route-rules
'[{"cidrBlock":"0.0.0.0/0","networkEntityId":"'$PRIVATE_IP_ID'"}]'
    fi
  ;;
  "backup") echo "Backup Status"
    logger "Backup Status"
    exit 0
    ;;
  "stop") echo "Keepalived stopped"
    logger "Keepalived stopped"
    exit 0
    ;;
  "fault") echo "Keepalived fault!"
    logger "Keepalived fault!" exit
    0
    ;;
  *)exit 1
    ;;
esac
```

付録2: keepalived.confの例

`${variable}`は実際の値に置き換えてください。

```
vrrp_instance VI_1 {
        interface ens3
        state MASTER

        virtual_router_id 51
        priority ${priority_map_1}

        unicast_src_ip ${private_ip}
        unicast_peer {
          ${peer_ip}
          ${peer2_ip}
        }

        notify_master "/usr/libexec/keepalived/notify.sh master ad1 ${ad1_rt_id}"
        notify_backup "/usr/libexec/keepalived/notify.sh backup ad1 ${ad1_rt_id}"
        notify_fault "/usr/libexec/keepalived/notify.sh fault ad1 ${ad1_rt_id}"
        notify_stop "/usr/libexec/keepalived/notify.sh stop ad1 ${ad1_rt_id}"

}

vrrp_instance VI_2 {
         interface ens3
         state BACKUP

         virtual_router_id 52
         priority ${priority_map_2}

         unicast_src_ip ${private_ip}
         unicast_peer {
           ${peer_ip}
           ${peer2_ip}
         }

        notify_master "/usr/libexec/keepalived/notify.sh master ad2 ${ad2_rt_id}"
        notify_backup "/usr/libexec/keepalived/notify.sh backup ad2 ${ad2_rt_id}"
        notify_fault "/usr/libexec/keepalived/notify.sh fault ad2 ${ad2_rt_id}"
        notify_stop "/usr/libexec/keepalived/notify.sh stop ad2 ${ad2_rt_id}"

}

vrrp_instance VI_3 {
         interface ens3
         state BACKUP

         virtual_router_id 53
         priority ${priority_map_3}

         unicast_src_ip ${private_ip}
         unicast_peer {
           ${peer_ip}
           ${peer2_ip}
         }

        notify_master "/usr/libexec/keepalived/notify.sh master ad3 ${ad3_rt_id}"
         notify_backup "/usr/libexec/keepalived/notify.sh backup ad3 ${ad3_rt_id}"
         notify_fault "/usr/libexec/keepalived/notify.sh fault ad3 ${ad3_rt_id}"
         notify_stop "/usr/libexec/keepalived/notify.sh stop ad3 ${ad3_rt_id}"

}
```

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

NATインスタンスの構成: プライベート・サブネットのインターネット・アクセスの有効化
2018年1月