

【初心者】AWS PrivateLink を使ってみる

AWS, PrivateLink

目的

- PrivateLinkは既に登場して2年ほどになる、ある程度枯れたサービスだが、構成を理解するため触ってみることにした。

AWS PrivateLink とは(自分の理解)

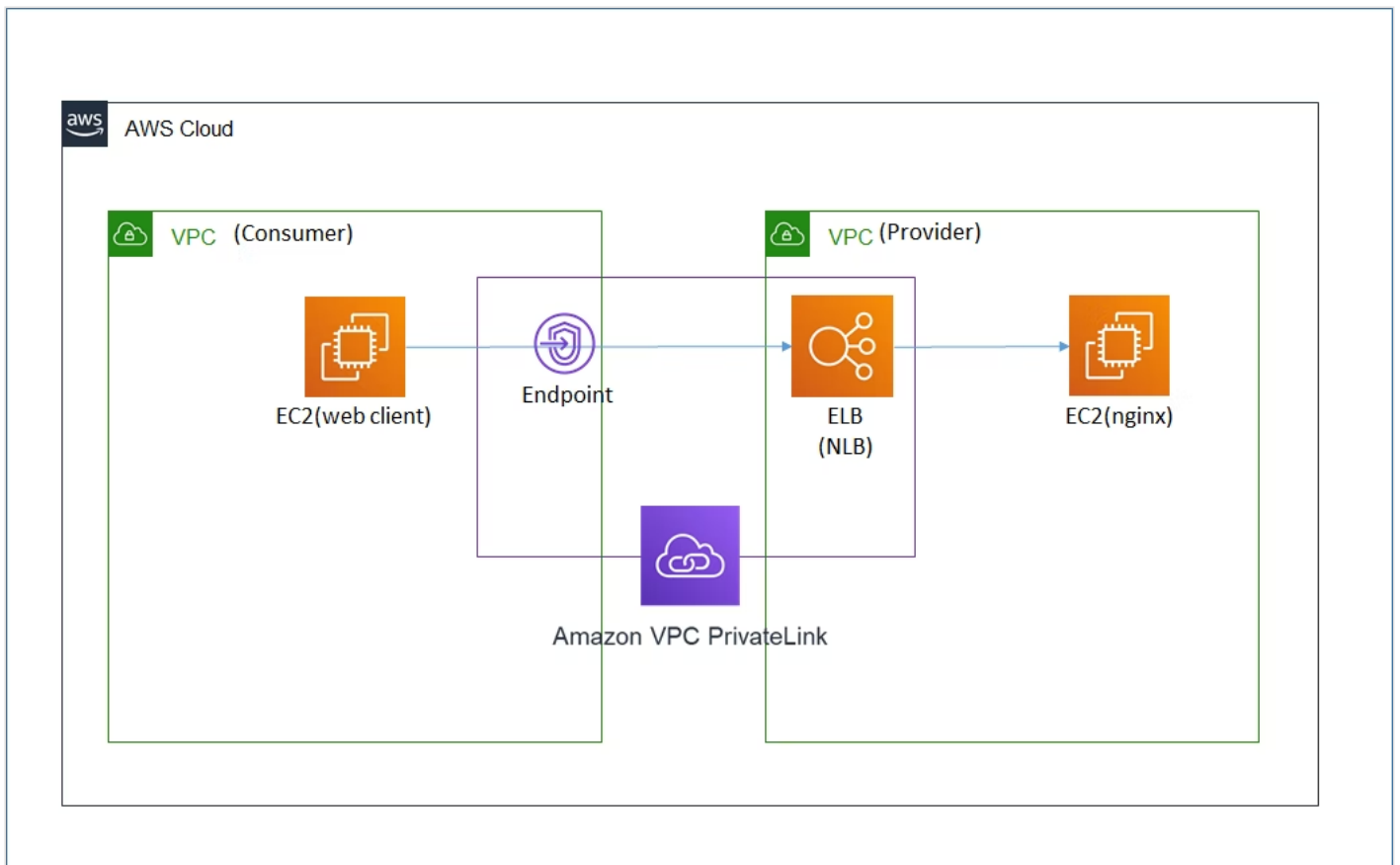
- 自分のVPCのNLB配下のWEB等のサービスを、同一リージョン内の他のVPCに公開できるサービス。VPCピアリング等と異なり、IPアドレスレンジの重複等の考慮が不要で、AWS内に閉じた安全なNW接続を実現できる。
- PrivateLinkは、サービスを公開する側（エンドポイントサービス）と、サービスにアクセスする側（インターフ

ェースエンドポイント) のセットで構成される。

やったこと

- VPC(Provider)側にNLBとEC2(nginx)、VPC(Consumer)側にEC2(WEB Client)を作成する。
- VPC(Provider)側で「エンドポイントサービス」を作成し、NLBを指定する。
- VPC(Consumer)側で「インターフェースエンドポイント」を作成し、接続先として、「エンドポイントサービス」を指定する。
- VPC(Provider)側で、「インターフェースエンドポイント」の接続要求を承認し、接続を確立する。
- EC2(web client)からEC2(nginx)へPrivateLink経由でhttpアクセスする。

構成図



作業手順


VPC(2個)及びEC2(WEBサーバ/クライアント)の作成

- VPC(Provider)を作成し、NLBとEC2(nginx)を作成する。
NLBのスキームを「内部」で設定する。

- VPC(Consumer)を作成し、EC2(WS2019,Web Client用)を作成する。

エンドポイントサービスの作成

- VPCのメニューから、「エンドポイントサービスの作成」を選択し、VPC(Provider側)にて既存のNLBを指定してエンドポイントサービスを作成する。「エンドポイントサービスの作成」とは、NLBの配下のサービスを、他のVPCに対しての公開サービスとして登録するイメージ。
2019/11現在、エンドポイントサービスとして公開設定できるのはNLBのみ。

 サービス リソースグループ

エンドポイントのサービス > エンドポイントサービスの作成

エンドポイントサービスの作成

PrivateLink テクノロジーを使用して、VPC のサービスを他の AWS アカウントおよびサービスで使用可能にできます。
PrivateLink は、サービスにプライベートアクセスできる可用性の高いスケーラブルなテクノロジーです。
他のアカウントおよびサービスが、お客様のエンドポイントサービスにアクセスするインターフェイスエンドポイントを作成できます。[詳細はこちら](#)。

Network Load Balancer の関連付け* mksamba-nlb 新規 Network Load Balancer を作成

属性によるフィルター、またはキーワードによる検索

Network Load Balancer	アベイラビリティゾーン
mksamba-nlb	ap-northeast-1a

含まれるアベイラビリティゾーン ap-northeast-1a (apne1-az4)

除外するアベイラビリティゾーン ap-northeast-1c (apne1-az1)
ap-northeast-1d (apne1-az2)

エンドポイントの承諾が必要 ☒ 承諾が必要

* 必須

キャンセル サービスの作成

インターフェースエンドポイントの作成

- VPCのメニューから、「エンドポイントの作成」を実行し、VPC(Consumer側)にてインターフェースエンドポイントを作成する。「インターフェースエンドポイント」は、「エンドポイントサービス」とつながる道の入口のようなもの。エンドポイントサービスの「サービス名」(com.amazonaws.vpce.ap-northeast-1.vpce-svc-

XXXXXXXXXXXXXXXXXXXX) を入力することで、エンドポイントサービスとの紐づけ要求を作成することができる。

aws

サービス ▾ リソースグループ ▾

エンドポイント > エンドポイントの作成

エンドポイントの作成

VPC エンドポイントを使用して、ご使用の VPC を他のサービスへ安全に接続できます。
インターフェイスエンドポイントには、[PrivateLink](#) が搭載されており、Elastic Network Interface (ENI) をサービス宛でのトラフィックのエントリーポイントとして使用します。
ゲートウェイエンドポイントは、サービスに対するトラフィックのルートテーブル内のルートのターゲットとして機能します。

サービスカテゴリ

☐ AWS サービス
☒ サービスを名前で検索
☐ ご使用の AWS Marketplace サービス

サービス名

プライベートサービス名を入力して確認します。 ⓘ

s.vpc.ap-northeast-1.vpc-svc-

サービス名が見つかりました。

検証

VPC*

vpc-

🔄 ⓘ

サブネット

subnet-

ⓘ

アベイラビリティゾーン	サブネット ID
<input checked="" type="checkbox"/> ap-northeast-1a (apne1-az4)	subnet- (mksamba-private-subnet2-tokyo2)
<input type="checkbox"/> ap-northeast-1c (apne1-az1)	このアベイラビリティゾーンではサポートされていないサービスです
<input type="checkbox"/> ap-northeast-1d (apne1-az2)	このアベイラビリティゾーンではサポートされていないサービスです

エンドポイントサービス側での承認

- エンドポイントサービス側の設定に戻ると、エンドポイントからの接続リクエストが「承諾の保留中」の状態になっているため、「エンドポイント接続リクエストの承

諾」を実行する。これにより、接続が確立される。

The screenshot shows the AWS Management Console interface for the 'Endpoints' page. The left sidebar contains a navigation menu with various AWS services. The main content area displays a table of endpoints. The table has columns for Name, ID, Type, Service Name, Status, and Availability. A single endpoint is listed with ID 'vpce-svc-...' and status 'Available'. Below the table, there is an 'Actions' dropdown menu that is open, showing options like 'Commit endpoint connection request' (エンドポイント接続リクエストの承諾) and 'Cancel endpoint connection request' (エンドポイント接続リクエストの却下). The 'Commit endpoint connection request' option is highlighted with a red box.

Name	ID	タイプ	サービス名	ステータス	アベイラビリティ
vpce-svc-		Interface	com.amazonaws.vpce.ap-northeast-1.vp...	Available	ap-northeast

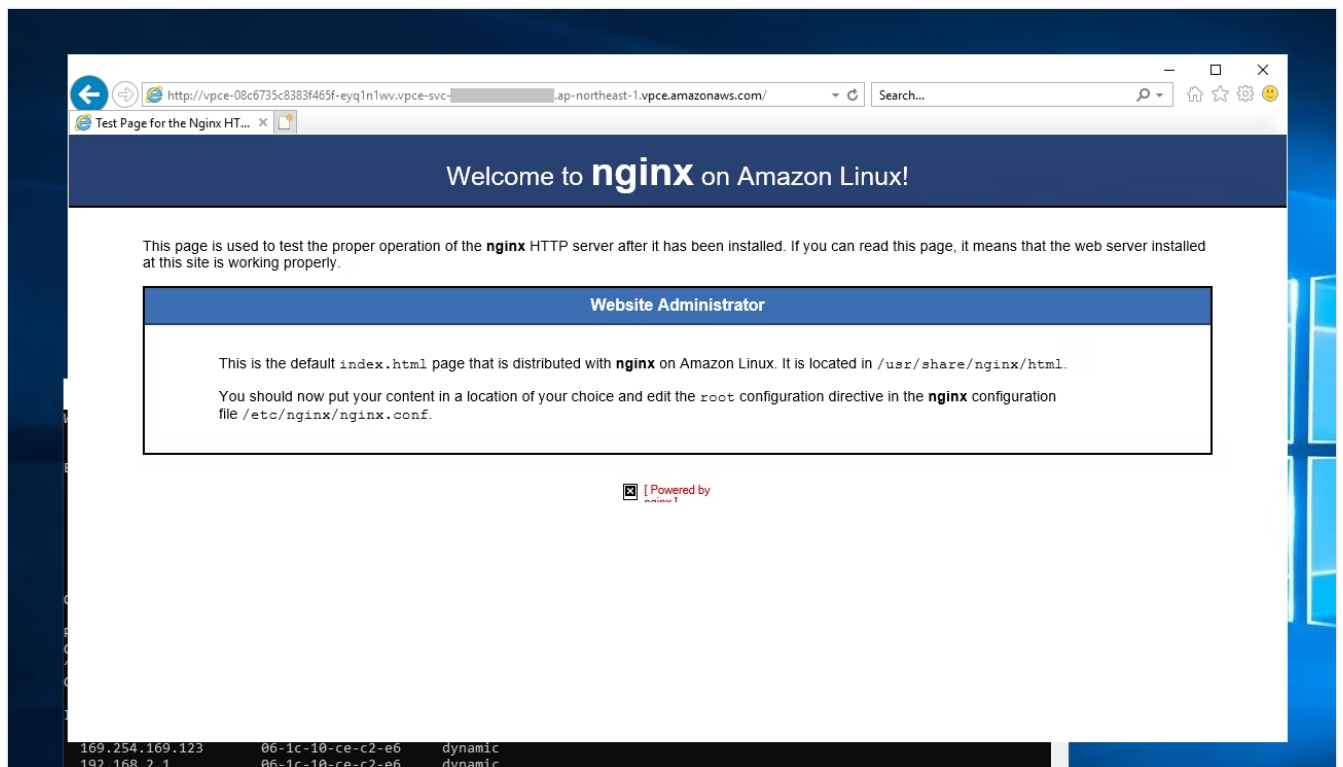
アクション
エンドポイント接続リクエストの承諾
エンドポイント接続リクエストの却下

エンドポイント ID	所有者	状態	作成日
vpce-		承諾の保留中	2019年11月13日 16:22:09 UTC+9

PrivateLink経由での接続確認

- VPC(Consumer)側で起動したEC2(WEB Client)のブラウザで、URLにインタフェースエンドポイントのDNS名を入力して、PrivateLink経由でNLBの先のEC2(nginx)へアクセス

スする。



所感

- VPC PrivateLinkというサービスメニューがあるわけではなく、「エンドポイントサービスとインターフェースエンドポイントをつなげること」＝「PrivateLink」という感じなので、ちょっと分かりにくいなと感じた。

参考

- 【新機能】 PrivateLinkで独自エンドポイントを作ってアプリをプライベート公開する #reinvent
 - ほとんどのこの記事の内容を実施して自分なりにまとめなおしただけ、、